数学名著译丛

抽象代数学

卷 3

域论及伽罗瓦理论

N. 贾柯勃逊 著

科学出版社

数学名著译丛

抽象代数学

卷 3
域论及伽罗瓦理论

N. 贾柯勃逊 著

李忠傧 俞曙霞 李世余 译



科学出版社
1987

内容简介

本书是作者根据他在几所大学里讲授的抽象代数学讲义编成的. 全书分三卷. 本卷是卷 3,主要叙述域论及伽罗瓦 (Galois) 理论, 是一本对于发展代数数论与代数几何具有重大价值的著作.

在这一卷中,作者阐述了理解近世代数数论、环论与代数几何学所需的主要基本域论的知识,着重讨论了有限维域扩张及伽罗瓦理论、域的一般结构理论、赋值论和关于阿贝尔 (Abel) 扩张的结果,同时指出了域的现代理论与引导它发展的古典问题之间的联系. 并论述了域论对分析学具有重要意义的部分.

本书可供数学研究工作者、高等院校数学系教师和学生参考.

N. Jacobson
LECTURES IN ABSTRACT ALGEBRA
III. THEORY OF FIELDS AND GALOIS THEORY
Springer-Verlag, 1964

数学名著译丛
抽象代数学
卷 3
域论及伽罗瓦理论

N. 贾柯勃逊 著
李忠傧 俞曙霞 李世余 译
责任编辑 苏芳霞

科学出版社出版
北京朝阳门内大街 137 号
中国科学院印刷厂印刷
新华书店北京发行所发行 各地新华书店经售
*
1987 年 8 月第 一 版 开本：850×1168 1/32
1987 年 8 月第一次印刷 印张：10 1/8
印数：0001—6,000 字数：265,000
统一书号：13031 · 3591
本社书号：5234 · 13—1
定价：2.90 元

序

本卷是著者十多年前开始编写的一套代数学教科书的最后一卷．这里所给出的域论及伽罗瓦[1]（Galois）理论是在本书第1卷中所出现的一般代数学概念与结果以及涉及线性代数的第2卷的较初等部分的基础上阐述的，本卷内容的深度大致与第2卷的相同．

在准备本书时我们曾作过多方面的考虑：首要的是编入基础域论，这是理解现代代数数论、环论及代数几何学所必需的．本卷涉及这个问题的部分是第一、四、五章，它们分别讨论有限维域扩张及伽罗瓦理论、域的一般结构理论和赋值论；还有第三章关于阿贝尔(Abel)扩张的结果，虽然看来专门了一些，但却是与数论密切相关的．我们的第二个目标是要指出域的现代理论与引导它发展的古典问题之间的联系，这一想法在第一章和第六章中得以实现，前者给出方程的根式可解性的伽罗瓦理论，后者给出阿廷（Artin）把实闭域理论用于正定有理函数上的希尔伯特（Hilbert）问题的解答．最后，我们还介绍域论对分析学具有重要意义的那些部分，这里特别值得注意的是我们在第六章所论述的实闭域里的多项式方程与不等式的塔尔斯基-赛登堡（Tarski-Seidenberg）判定法．

同前两卷书一样，习题也构成本卷的重要部分，其中有少部分是十分困难的．

在这里，我要向我的朋友们致谢：P. 柯恩（P. Cohn）与 G. 西利曼（G. Seligman）教授细心审阅了初稿，本卷采纳了他们的很多建议；我还感谢柯恩和 J. 莱特（J. Reid）教授以及我的妻

1）在第一卷和第二卷中，"Galois"一词均译为"加罗华"，本卷按目前习惯，译为"伽罗瓦"——译者注．

予帮助校对本书．最后，对于美国空军科学发展局给予的长达一个夏季和半个学年的大力支持表示感谢，这一支持使本书能较原计划提前完成。

贾柯勃逊（N. Jacobson）

New Haven, Conn.

1964年1月20日

目 录

导　言

本书假定读者已熟悉卷 1 中所出现的代数学的一般概念和域的结果以及卷 2 的较初等部分．特别地，我们假定读者已具有域的特征、素域、交换整区的分式域的构造法以及域的单代数扩张与单超越扩张的构造法等知识，这些概念在卷 1 的第二、三章介绍过．我们还需要第四章的因式分解的初等理论．在卷 2 中，我们需要域上的向量空间、维数、线性变换、线性函数、线性变换的合成、双线性型等基本概念．但线性变换及双线性型的标准形等较高深结果却不是必要的．

在这个导言中我们将复习前面已经讲过的一些内容，这有双重意义：首先，强调以前的一些结果对今后的使用是有利的；其次，为了方便查阅，所以将今后经常用到的一些结果列举出来．这里要讨论的主题有：同态的扩张(参看卷 1，第三章)、代数(卷 2，第七章)以及向量空间和代数的张量积[1](卷 2，第七章)．同态的扩张这一概念在域论中是一个重要的工具；代数的概念是在研究一个域以一个选定的子域为其基域时自然产生的；本来张量积的概念在域论中不怎么重要，我们完全可以避开它，然而，这个概念近年来在整个代数学及代数拓朴学中却显得非常重要，所以对于学生来说，熟练掌握张量积是十分必要的．在适当场合我们将要自由地运用它．

1. 同态的扩张　我们约定：本书中所考虑的环都有单位元 $1\neq 0$，从而子环一词将仍如卷 1 那样表示包含 1 的子环，而环 $\mathfrak{A}$ 到环 $\mathfrak{B}$ 内的同态我们将理解为在旧意义下的将 $\mathfrak{A}$ 的 1 映到 $\mathfrak{B}$ 的

1) 在卷 2 中此概念原称为克罗内克 (Kronecker) 积，但近来常爱用张量积一词，所以我们在本卷中将采用这个名词，而且将使用近代标准符号⊗来代替卷 2 中的×．——著者注．

1 的同态.

现设 $\mathfrak{o}$ 为域 P 的子环而 Φ 为 P 的由 $\mathfrak{o}$ 生成的子域. 我们知道, Φ 的元能表成简单分式 $\alpha\beta^{-1}$, 这里的元 $\alpha, \beta \in \mathfrak{o}(\beta \neq 0)$. 因此 Φ 是 P 的一个子环, 它是由 $\mathfrak{o}$ 及 $\mathfrak{o}$ 的非零元的逆元生成的, 我们将 $\mathfrak{o}$ 的非零元集用 $\mathfrak{o}^*$ 表示, 则集 $\mathfrak{o}^*$ 包含 1 且关于 $\mathfrak{o}$ 的乘法封闭. 有时将此情况作如下的推广是有益的: 设已给定 P 的一个子环 $\mathfrak{o}$ 及 $\mathfrak{o}^*$ 的一个子集 M, 它包含 1 且关于乘法封闭, 我们把这样的一个子集称为域的乘法群的子半群. 我们感兴趣的是由 $\mathfrak{o}$ 及 M 的元的逆元生成的子环 $\mathfrak{o}_M$. 例如, 我们可取 P 为有理数域 R_0 而 $M = \{2^k | k = 0, 1, 2, \cdots\}$, 则 $\mathfrak{o}_M$ 是分母为 2 的方幂的有理数子环. 一般情况是

$$\mathfrak{o}_M = \{\alpha\beta^{-1} | \alpha \in \mathfrak{o}, \beta \in M\};$$

因为, 如果将这个等式的右端的集合表为 $\mathfrak{o}'$, 则显然 $\mathfrak{o}' \subseteq \mathfrak{o}_M$, 而 $\mathfrak{o}'$ 包含 $\mathfrak{o} = \{\alpha = \alpha 1^{-1}\}$. 对于 $\beta \in M$, $\mathfrak{o}'$ 也包含每个 $\beta^{-1} = 1\beta^{-1}$. 可以直接验证 $\mathfrak{o}'$ 是 P 的一个子环, 故得 $\mathfrak{o}' = \mathfrak{o}_M$.

设 P′ 是第二个域且有 $\mathfrak{o}$ 到 P′ 内的一个同态 s; 它对于每个 $\beta \in M$ 总有 $\beta^s \neq 0$. 我们的第一个同态扩张定理就是关于这种情况的, 其结果是:

I 设 $\mathfrak{o}$ 是域 P 的(含有 1) 一个子环, M 是 $\mathfrak{o}$ 的一个非零元的子集, 它包含 1 且关于乘法封闭, $\mathfrak{o}_M$ 是 $\mathfrak{o}$ 及 M 的元的逆元所生成的 P 的子环, 设 s 是 $\mathfrak{o}$ 到域 P′ 内的一个同态, 它对每个 $\beta \in M$ 都有 $\beta^s \neq 0$, 则 s 能唯一地扩张成 $\mathfrak{o}_M$ 到 P′ 内的同态 S. 此外, S 是一个同构, 当且仅当 s 是一个同构.

证 设 $\alpha_1\beta_1^{-1} = \alpha_2\beta_2^{-1}$, $\alpha_i \in \mathfrak{o}$, $\beta_i \in M$, 则 $\alpha_1\beta_2 = \alpha_2\beta_1$, 从而 $\alpha_1^s\beta_2^s = \alpha_2^s\beta_1^s$. 这个关系在 P′ 中给出 $\alpha_1^s(\beta_1^s)^{-1} = \alpha_2^s(\beta_2^s)^{-1}$. 因此定义在整个 $\mathfrak{o}_M = \{\alpha\beta^{-1}\}$ 上的映射

$$S: \alpha\beta^{-1} \to \alpha^s(\beta^s)^{-1}, \quad \alpha \in \mathfrak{o}, \ \beta \in M$$

是单值的. 可以验证 S 是一个同态 (卷 1 中译本 p.86). 今取 $\alpha \in \mathfrak{o}$, 则 $\alpha^S = (\alpha 1^{-1})^S = \alpha^s 1^s = \alpha^s$, 因此 S 在 $\mathfrak{o}$ 上是与 s 相同的. 故 S 是 $\mathfrak{o}_M$ 的一个同态, 它是由 $\mathfrak{o}$ 的已知同态扩张而成的. 现

设 S' 是任一这样的扩张，则对于 $\beta\in M$，关系 $\beta\beta^{-1}=1$ 将给出 $\beta^{S'}(\beta^{-1})^{S'}=1$，因此 $(\beta^{-1})^{S'}=(\beta^{S'})^{-1}$。若 $\alpha\in\mathfrak{o}$，则有 $(\alpha\beta^{-1})^{S'}=\alpha^{S'}(\beta^{S'})^{-1}=\alpha^{s}(\beta^{s})^{-1}=(\alpha\beta^{-1})^{S}$，因此 $S'=S$，故 S 是唯一的。显然，若 S 是一个同构，则它在 $\mathfrak{o}$ 上的限制 s 也是一个同构。现设 s 是一个同构，且设 $\alpha\beta^{-1}$ 属于同态 S 的核：

$$0=(\alpha\beta^{-1})^{S}=\alpha^{s}(\beta^{s})^{-1},$$

则 $\alpha^{s}=0$，$\alpha=0$ 及 $\alpha\beta^{-1}=0$。这表示 S 的核是 0；因此 S 是一个同构。

其次考虑任一交换环 $\mathfrak{A}$ 及多项式环 $\mathfrak{A}[x]$，x 是关于 $\mathfrak{A}$ 的超越元(卷1，中译本 p.87)。$\mathfrak{A}[x]$ 的元形如

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n,$$

其中 $a_i\in\mathfrak{A}$，而且仅当所有的 $a_i=0$ 时 $a_0+a_1x+\cdots+a_nx^n=0$。于是我们有如下的同态定理：

II 令 $\mathfrak{A}$ 是一个交换环，$\mathfrak{A}[x]$ 是 $\mathfrak{A}$ 上的超越元 x 的多项式环，且 s 是 $\mathfrak{A}$ 到交换环 $\mathfrak{B}$ 内的同态，若 u 是 $\mathfrak{B}$ 的任一元，则必存在唯一的 $\mathfrak{A}[x]$ 到 $\mathfrak{B}$ 内的同态 S 使

$$a^{S}=a^{s},\ a\in\mathfrak{A},\ x^{S}=u.$$

对于这个证明读者可参看卷1(中译本 p.89)。此结果可直接扩广到多项式环 $\mathfrak{A}[x_1,x_2,\cdots,x_r]$，这里的 x_i 是代数无关元，而 x_i 的代数无关性指的是：若 $(m_1,m_2,\cdots,m_r)$ 是非负整数 m^i 的 r 数组，则关系 $\sum\limits_{m_i}a_{m_1\cdots m_r}x_1^{m_1}\cdots x_r^{m_r}=0$ $(a_{m_1\cdots m_r}\in\mathfrak{A})$ 仅当每个 $a_{m_1\cdots m_r}=0$ 时成立。今后我们把属于交换环而关于子环 $\mathfrak{A}$ 为代数无关的元 x_i 称为(关于 $\mathfrak{A}$ 的)未定元。我们有

III 设 $\mathfrak{A}[x_1,\cdots,x_r]$ 是（关于 $\mathfrak{A}$ 的）未定元 x_i 的交换多项式环，s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个同态，若 $u_1,u_2,\cdots,u_r$ 是 $\mathfrak{B}$ 的任意元，则存在唯一的 $\mathfrak{A}[x_i]$ 到 $\mathfrak{B}$ 内的同态 S 使 1)$a^{S}=a^{s}$，$a\in\mathfrak{A}$；2)$x_i^{S}=u_i$，$i=1,2,\cdots,r$。

现在我们假定有一个交换环 $\mathfrak{C}$，$\mathfrak{A}$ 是它的一个子环，s 是 $\mathfrak{A}$ 到另一交换环 $\mathfrak{B}$ 内的同态。设 $t_1,t_2,\cdots,t_r$ 是 $\mathfrak{C}$ 的元而 $\mathfrak{A}[t_1,t_2,\cdots,$

t_r] 是由 $\mathfrak{A}$ 及 t_i 生成的 $\mathfrak{C}$ 的子环. 我们问: 在什么条件下能使 s 扩张成一个 $\mathfrak{A}[t_i]=\mathfrak{A}[t_1, t_2, \cdots, t_r]$ 到 $\mathfrak{B}$ 内的同态 S 使 $t_i^S=u_i$, $1\leqslant i\leqslant r$, 其中 u_i 是 $\mathfrak{B}$ 的预先指定的元? 这个基本问题的回答是:

IV 令 $\mathfrak{B}$ 及 $\mathfrak{C}$ 都是交换环, $\mathfrak{A}$ 是 $\mathfrak{C}$ 的一个子环, s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个同态, $t_1, t_2, \cdots, t_r$ 是 $\mathfrak{C}$ 的元, $u_1, u_2, \cdots, u_r$ 是 $\mathfrak{B}$ 的元, 则存在一个 $\mathfrak{A}[t_1, \cdots, t_r]$ 到 $\mathfrak{B}$ 内的同态 S 使 $a^S=a^s$ $(a\in\mathfrak{A})$ 及 $t_i^S=u_i(i=1, 2, \cdots, r)$, 当且仅当对于每个多项式 $f(x_1, \cdots, x_r)\in\mathfrak{A}[x_i]$ (x_i 是未定元) 都有: 若 $f(t_1, \cdots, t_r)=0$, 则 $f^s(u_1, \cdots, u_r)=0$, 这里 $f^s(x_1, \cdots, x_r)$ 是将 s 作用在 $f(x_1, \cdots, x_r)$ 的系数上而得到的. 若 S 存在, 则它是唯一的.

证. 使 $f(t_1, \cdots, t_r)=0$ 的多项式 $f(x_1, \cdots, x_r)$ 的集 $\mathfrak{K}$ 是 $\mathfrak{A}[x_i]$ 到 $\mathfrak{A}[t_i]$ 内的同态 $h(x_1, \cdots, x_r)\to h(t_1, \cdots, t_r)$ 的核, 因此我们有 $\mathfrak{A}[t_i]$ 到差环 $\mathfrak{A}[x_i]/\mathfrak{K}$ 上的同构 $\tau: h(t_1, \cdots, t_r)\to h(x_1, \cdots, x_r)+\mathfrak{K}$. 然后考虑 $\mathfrak{A}[x_i]$ 到 $\mathfrak{B}$ 内的同态 $h(x_1, \cdots, x_r)\to h^s(u_1, \cdots, u_r)$ (参考 III). 假定对于每个 $f\in\mathfrak{K}$ 都有 $f^s(u_1, \cdots, u_r)=0$, 则每个 $f\in\mathfrak{K}$ 都被同态 $h(x_1, \cdots, x_r)\to h^s(u_1, \cdots, u_r)$映入到0, 因此 $\mathfrak{K}$ 含于此同态的核中, 从而(参看卷 1 中译本 p.67)我们有$\mathfrak{A}[x_i]/\mathfrak{K}$ 到 $\mathfrak{B}$ 内的同态$h(x_1, \cdots, x_r)+\mathfrak{K}\to h^s(u_1, \cdots, u_r)$. 把它与同构 τ 结合就得到 $\mathfrak{A}[t_i]$ 到 $\mathfrak{B}$ 内的同态

$$S: h(t_1, \cdots, t_r)\to h^s(u_1, \cdots, u_r), \tag{1}$$

这就是所要求的 s 的扩张. 若 S' 是 s 的由 $\mathfrak{A}[t_i]$ 到 $\mathfrak{B}$ 内的同态的任一扩张, 它使 $a^{S'}=a^s$ 及 $t_i^{S'}=u_i$, 则 $h(t_1, \cdots, t_r)^{S'}=h^s(u_1, \cdots, u_r)$; 因此 $S'=S$. 故 S 是唯一的. 显然还有: 若 S 是 $\mathfrak{A}[t_1, \cdots, t_r]$ 的一个满足条件的同态, 那么由 $f(t_1, \cdots, t_r)=0$ 必有 $0=f(t_1, \cdots t_r)^S=f^s(u_1, \cdots, u_r)$. 显然可见定理中的条件是存在扩张 S 所必须的.

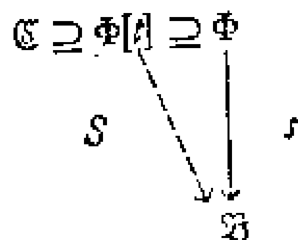
我们在定理的证明中曾经指出, 使 $f(t_1, \cdots, t_r)=0$ 的多项式 $f(x_1, \cdots, x_r)$ 的集 $\mathfrak{K}$ 是同态的核, 因此它是多项式环 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 中的一个理想. 令 $X=\{g\}$ 为 $\mathfrak{K}$ 的一个生成元集:

$X \subseteq \mathfrak{K}$，则每个元 $f \in \mathfrak{K}$ 可表成 $\sum a_i(x_1, \cdots x_r) g_i(x_1, \cdots, x_r)$，这里 $a_i(x_1, \cdots, x_r) \in \mathfrak{A}[x_1, x_2, \cdots, x_r]$，而 $g_i(x_1, \cdots, x_r) \in X$. 显然可见：如果 $g^s(u_1, \cdots, u_r) = 0$ 对每个 $g \in X$ 成立，则 $f^s(u_1, \cdots, u_r) = 0$ 也对每个 $f \in \mathfrak{K}$ 成立，因而我们可以从 IV 得到一个较 IV 更便于应用的下述结果：

IV′ 令 $\mathfrak{B}$ 及 $\mathfrak{C}$ 为交换环，$\mathfrak{A}$ 为 $\mathfrak{C}$ 的一个子环，s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个同态，X 是 $\mathfrak{A}[x_1, x_2, \cdots, x_r]$ 中适合条件 $f(t_1, t_2, \cdots, t_r) = 0$ 的多项式 f 构成的理想 $\mathfrak{K}$ 的生成元集，其中 x_i 为未定元，则当且仅当对于每个 $g \in X$ 都有 $g^s(u_1, \cdots, u_r) = 0$ 时，存在一个 $\mathfrak{A}[t_1, t_2, \cdots, t_r]$ 到 $\mathfrak{B}$ 内的同态 S 使 $a^S = a^s (a \in \mathfrak{A})$，$t_i^S = u_i \ (1 \leqslant i \leqslant r)$. 若 S 存在，则它是唯一的.

现考虑 IV′ 的一个重要特殊情况：$\mathfrak{A} = \Phi$ 是一个域且 $r = 1$. 我们知道这时的 $\Phi[x]$ 是一个主理想整区（卷 1 的中译本 p.93），所以此理想 $\mathfrak{K} = (f(x))$，这里 $(f(x))$ 表示多项式 $f(x) \in \mathfrak{K}$ 的多项式倍式构成的理想. 显然 $\mathfrak{K} \neq 1 = \Phi[x]$，因若不然，将有 $0 = \Phi[x]/\mathfrak{K} \cong \Phi[t] \supseteq \Phi$，而这是与 $1 \neq 0$ 矛盾的. 因为如果 α 是 Φ 的非零元时有 $(\alpha) = (1)$，显然 $\mathfrak{K}$ 只能有两种可能，即 $\mathfrak{K} = (0)$ 或者 $\mathfrak{K} = (f(x))$，这里的 $f(x)$ 是 $\Phi[x]$ 中的一个非零的正次数多项式. 在第一种情况，我们有 $\Phi[x] \cong \Phi[t]$，而 t 是超越元. 这时应用 II（或 IV）就能将 s 扩张成将 t 映入到任一 $u \in \mathfrak{B}$ 的一个同态 S. 现设 $f(x) \neq 0$，在这一情况下，我们称元 $t \in \mathfrak{C}$ 为 Φ 上的代数元，这是因为我们有非零多项式 $f(x)$ 使 $f(t) = 0$. 由定义，理想 $\mathfrak{K}$ 是使 $g(t) = 0$ 的多项式 $g(x)$ 的集. 多项式 $f(x)$ 是 $\mathfrak{K}$ 中次数最低的一个多项式，而含于 $\mathfrak{K} = (f(x))$ 之中的每个其它多项式的形式为 $g(x)f(x)$. 用 $f(x)$ 的首项系数的逆元乘 $f(x)$，就能将 $f(x)$ 正规化为首项系数为 1 的多项式. 令 $f(x)$ 为这个多项式，则 f 显然可用下列性质来刻划：它是 $\Phi[x]$ 的、首项系数为 1 的、满足 $f(t) = 0$ 的最低次数多项式，我们将称 $f(x)$ 为（Φ 上的）代数元 $t \in \mathfrak{C}$ 的最小多项式. 对于 IV′ 的这种特殊情况，有如下结论：

V 设 $\mathfrak{B}$ 及 $\mathfrak{C}$ 为交换环，Φ 为 $\mathfrak{C}$ 的子域，$t\in\mathfrak{C}$ 是 Φ 上的代数元，s 是 Φ 到 $\mathfrak{B}$ 内的一个同构：



则 s 可扩张成 $\Phi[t]$ 到 $\mathfrak{B}$ 内的一个同态 S 使 $t^S=u$，当且仅当对于 Φ 上的 t 的最小多项式 $f(x)$ 有 $f^s(u)=0$. 若此扩张存在，则它是唯一的.

附注 保证 S 存在的附加在 u 上的条件也可改用下列方式表述：u 是 Φ 的象 Φ^s 上的代数元，它在 Φ^s 上的最小多项式是 $f^s(x)$ 的一个因式，关于 S 的(1)式现变为

$$S:\ g(t)\to g^s(u). \tag{2}$$

由此易得：S 是一个同构当且仅当 $f^s(x)$ 是 u 的最小多项式.

2. 代数 现在来回顾域 Φ 上的代数 $\mathfrak{A}$ 的定义（卷 2 的中译本 p.32 及 p.201）：$\mathfrak{A}$ 是 Φ 上的向量空间，而且对于 $\mathfrak{A}$ 中的任意元 x, y 定义了一个"乘积" $xy\in\mathfrak{A}$，使得

$$\begin{aligned}&(x_1+x_2)y=x_1y+x_2y,x(y_1+y_2)=xy_1+xy_2\\&\alpha(xy)=(\alpha x)y=x(\alpha y)\quad(\alpha\in\Phi).\end{aligned}\tag{3}$$

我们关心的仅是有单位元 1 且可结合的代数，因此本卷中的"代数"仅限于这种.

我们经常遇到以下述方式出现的代数：给定一个环 $\mathfrak{A}$ 及 $\mathfrak{A}$ 的中心的一个子域 Φ，我们就可以把 $\mathfrak{A}$ 看成是 Φ 上的向量空间，这只要把 $\alpha x(\alpha\in\Phi,\ x\in\mathfrak{A})$ 按照 α 与 x 在 $\mathfrak{A}$ 中的环的乘积规定就行了. 显然这能使 $\mathfrak{A}$ 成为 Φ 上的向量空间. 由于 α 属于环 $\mathfrak{A}$ 的中心，(3)是显然成立的. 因此我们有代数 $\mathfrak{A}/\Phi$（Φ 上的 $\mathfrak{A}$）[1].

---

1) 我们还用记号 $\mathfrak{A}/\mathfrak{B}$ 表示 $\mathfrak{A}$ 关于理想 $\mathfrak{B}$ 的差环，但它们是很容易从前后文区分开来的. ——译者注

这种定义代数的方法将被应用到域P关于它的子域Φ的研究，这时就得到代数 P/Φ.

另一基本的代数是域 Φ 上的向量空间 $\mathfrak{M}$ 的线性变换代数 $\mathfrak{L}_\Phi(\mathfrak{M})$，这里对于 $A, B \in \mathfrak{L}_\Phi(\mathfrak{M})$ 及 $\alpha \in \Phi$, $A + B$, AB 及 αA 的定义是： $x(A+B) = xA + xB$, $x(AB) = (xA)B$, $x(\alpha A) = \alpha(xA) = (\alpha x)A$. $\mathfrak{L}_\Phi(\mathfrak{M})$ 关于Φ的维数 $[\mathfrak{L}_\Phi(\mathfrak{M}):\Phi]$ 有限当且仅当 $[\mathfrak{M}:\Phi]$ 有限. 若 $[\mathfrak{M}:\Phi] = m$, 则 $[\mathfrak{L}_\Phi(\mathfrak{M}):\Phi] = m^2$ (卷 2 的中译本 p.36).

显然一个代数对于向量空间的加法 $a + b$ 及乘法 ab 来说是一个环. Φ 上的代数 $\mathfrak{A}$ 的一个**子代数** $\mathfrak{B}$ 是 $\mathfrak{A}$ 的一个子空间而且也是它的一个子环. $\mathfrak{A}/\Phi$ 的一个**理想**是一个子空间，且在将 $\mathfrak{A}$ 看作环时，它是 $\mathfrak{A}$ 的一个理想. 代数 $\mathfrak{A}/\Phi$ 到代数 $\mathfrak{B}/\Phi$ 内的一个**同态** s 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一个映射，它是Φ线性的而且是环同态的. 同构与自同构可类似地定义. 若 $\mathfrak{K}$ 是 $\mathfrak{A}/\Phi$ 的一个理想，则商空间 $\mathfrak{A}/\mathfrak{K}$ 关于它的向量空间的合成及乘法 $(a+\mathfrak{K})(b+\mathfrak{K}) = ab + \mathfrak{K}$ 来说是Φ上的代数. 我们有由 $\mathfrak{A}/\Phi$ 到 $\mathfrak{A}/\mathfrak{K}$ 上的关于Φ的代数同态 $a \to a + \mathfrak{K}$. 若 s 是 $\mathfrak{A}/\Phi$ 到 $\mathfrak{B}/\Phi$ 内的同态，则象 $\mathfrak{A}^s$ 是 $\mathfrak{B}$ 的一个子代数且 s 的核 $\mathfrak{K}$ 是 $\mathfrak{A}$ 的一个理想. 我们有 $\mathfrak{A}/\mathfrak{K}$ 到 $\mathfrak{A}^s$ 上的同构 $a + \mathfrak{K} \to a^s$. 关于环同态的基本结果可以推广到代数，我们将直接应用它们而不另作声明.

我们现在将一些今后常用的有限维代数的基本结果写在下面. 第一个涉及 $\mathfrak{A}/\Phi$ 及 $\mathfrak{A}/E$ 的维数关系，这里E是Φ的子域. 若E是Φ的一个子域，则我们可以将乘法 $\alpha x (\alpha \in \Phi, x \in \mathfrak{A})$ 中的 α 限制在E里面，这就将 $\mathfrak{A}$ 变成E上的代数 $\mathfrak{A}$. 还因为E是Φ的一个子域，我们可以定义代数 Φ/E. 于是有

VI **设 $\mathfrak{A}$ 为Φ上的代数，E为Φ的一个子域，若** $[\mathfrak{A}:\Phi] < \infty$ **及** $[\Phi:E] < \infty$, **则**

$$[\mathfrak{A}:E] = [\mathfrak{A}:\Phi][\Phi:E] \tag{4}$$

证 设 (u_i) $(1 \leqslant i \leqslant n)$ 为$\mathfrak{A}/\Phi$ 的一个基，$(\gamma_j)(1 \leqslant j \leqslant m)$ 为 Φ/E 的一个基，我们若能证明 $(\gamma_j u_i)$ 是 $\mathfrak{A}/E$ 的一个基，

则就证明了(4)．先令 $a\in\mathfrak{A}$，则 $a=\sum_{1}^{n}\alpha_i u_i(\alpha_i\in\Phi)$，又因 $\alpha_i=\sum_{j=1}^{m}\varepsilon_{ij}\gamma_j(\varepsilon_{ij}\in E)$，所以 $a=\sum\varepsilon_{ij}\gamma_j u_i$ 是系数 ε_{ij} 在 E 中的元 $\gamma_j u_i$ 的一个线性组合．现设 $\sum\varepsilon_{ij}\gamma_j u_i=0\ (\varepsilon_{ij}\in E)$，亦即 $\sum\alpha_i u_i=0\ \left(\alpha_i=\sum_j\varepsilon_{ij}\gamma_j\in\Phi\right)$．因为 u_i 是 Φ 无关的，故 $\alpha_i=0(1\leqslant i\leqslant n)$．再由公式 $\alpha_i=\sum\varepsilon_{ij}\gamma_j$ 及 γ_j 的 E 无关性得到：对于一切 i，j，$\varepsilon_{ij}=0$．这就证明了元素 $\gamma_j u_i$ 是 E 无关的，从而它们是 $\mathfrak{A}/E$ 的一个基．

VII 若 $\mathfrak{A}$ 是域 Φ 上的一个有限维代数，则 $\mathfrak{A}$ 是一个可除环当且仅当 $\mathfrak{A}$ 是一个整区．

证 我们知道除环必为整区（卷 1 的中译本 p.53）．现设 $\mathfrak{A}$ 是一个整区而 a 是 $\mathfrak{A}$ 的任一非零元，考虑被 a 决定的右乘映射 a_R: $x\to xa$，这是 $\mathfrak{A}/\Phi$ 中的一个线性变换，而且因为在 $\mathfrak{A}$ 中由 $ba=0$ 可推出 $b=0$，a_R 的零空间为 0，因而 a_R 是满射（即 $\mathfrak{A}$ 到 $\mathfrak{A}$ 上的映射），因此存在一个元 a' 使 $a'a=a'a_R=1$，即 a 有一左逆元；利用左乘映射作类似的推导可得 a 有一右逆元．因此 $\mathfrak{A}$ 的每个非零元都是一个单位，从而 $\mathfrak{A}$ 是一个可除环．

其次我们考虑有单个生成元 t 的代数 $\mathfrak{A}=\Phi[t]$（参考 §1）．我们有 $\Phi[x]$（这里 x 是未定元）到 $\mathfrak{A}$ 上的同态 $g(x)\to g(t)$．若 $\mathfrak{R}$ 是它的核，则 $\mathfrak{A}\cong\Phi[x]/\mathfrak{R}$．我们在 §1 中还证明过 $\mathfrak{R}=(f(x))$，这里 $f(x)=0$ 或是一个首项系数为 1 的非零多项式．在第一种情况，t 是超越元而所给的同态是一个同构；在第二种情况，t 是代数元而 $f(x)$ 是它的最小多项式．因此我们有：

VIII 令 $\mathfrak{A}=\Phi[t]$ 是 Φ 上的由单个代数元 t 生成的代数，其最小多项式为 $f(x)$，则

(5) $$[\mathfrak{A}:\Phi]=\deg f(x),$$

这里，$\deg f(x)$ 表示 $f(x)$ 的次数．

证 令 $n=\deg f(x)$，我们可断言 $(1,t,\cdots,t^{n-1})$ 是 $\mathfrak{A}/\Phi$

的一个基. 若令 a 为 $\mathfrak{A}=\Phi[t]$ 的任一元,那么它就有多项式形式 $g(t)$, 这里 $g(x)$ 是 $\Phi[x]$ 中的多项式. 由 $\Phi[x]$ 中的除法可得 $g(x)=f(x)q(x)+r(x)$, 这里的 $\deg r(x)<\deg f(x)$. 因此若利用 $\Phi[x]/\Phi$ 到 $\Phi[t]/\Phi$ 上的将 x 变为 t 的同态,我们就可得到 $a=g(t)=0\,q(t)+r(t)$. 由于 $\deg r(x)<n$, 这表示 $a=r(t)$ 是 $1, t, \cdots, t^{n-1}$ 的一个 Φ 线性组合. 其次我们还应注意 $1, t, \cdots, t^{n-1}$ 关于 Φ 是线性无关的(否则我们将有一个次数 $<n$ 的多项式 $g(x)\neq 0$ 使 $g(t)=0$, 这与 $f(x)$ 是最小多项式的假设矛盾). 故 $(1, t, \cdots, t^{n-1})$ 是一个基,因而(5)成立.

我们知道, $\Phi[t]\cong\Phi[x]/(f(x))$ ($f(x)$ 是一个正次数多项式)是一个域当且仅当 $f(x)$ 是不可约的(卷 1 的中译本 p.96),否则 $\Phi[t]$ 不是一个整区、利用最小多项式 $f(x)$ 对 $\Phi[t]$ 的结构作一个完备的分析是很有用的, 在下面习题中我们将指出这些结果.

习　　题　　1

1. 代数 $\mathfrak{A}$ 是理想 $\mathfrak{A}_i$ 的一个直和, 如果 $\mathfrak{A}$ 是子空间 $\mathfrak{A}_i$ 的向量空间的直和. $\mathfrak{A}=\Phi[t]$, t 是最小多项式为 $f(x)$ 的代数元. 假设 $f(x)=f_1(x)f_2(x)\cdots f_r(x)$, 这里的 $(f_i(x), f_j(x))=1\,(i\neq j)$. 今令 $q_i(x)=f(x)/f_i(x)$, 证明存在多项式 $a_i(x)$ 使得

$$\sum_1^r a_i(x)q_i(x)=1.$$

令 $e_i=a_i(t)q_i(t)$, 证明

$$e_1+e_2+\cdots+e_r=1,\ e_i^2=e_i,\ e_ie_j=0,\ i\neq j.$$

并证明 $\mathfrak{A}=\mathfrak{A}e_1\oplus\mathfrak{A}e_2\oplus\cdots\oplus\mathfrak{A}e_r$, 而且在将理想 $\mathfrak{A}e_i=\{ae_i \mid a\in\mathfrak{A}\}$ 作为有单位元 e_i 的一个代数考虑时有形式 $\Phi[te_i]$, 并与 $\Phi[x]/(f_i(x))$ 同构.

2. 设 $\mathfrak{A}=\Phi[t]$, t 是最小多项式为 $f(x)$ 的代数元. 设 $f(x)=p_1(x)^{k_1}p_2(x)^{k_2}\cdots p_r(x)^{k_r}$, $p_i(x)$ 是不可约多项式, $p_i(x)\neq p_j(x)$, $i\neq j$. 证明, 若 $z=p_1(t)p_2(t)\cdots p_r(t)$, 则 $\mathfrak{A}$ 的理想 $\mathfrak{N}=\mathfrak{A}z$ 在下述意义下是幂零的: 存在一个整数 k, $\mathfrak{N}$ 中任意 k 个元的积均为 0. 证明: $\bar{\mathfrak{A}}=\mathfrak{A}/\mathfrak{N}=\Phi[\bar{t}]$, $\bar{t}=t+\mathfrak{N}$, $\bar{t}$ 是最小多项式为 $g(x)=p_1(x)p_2(x)\cdots p_r(x)$ 的代数元. 证明: $\bar{\mathfrak{A}}=\bar{\mathfrak{A}}_1\oplus\bar{\mathfrak{A}}_2\oplus\cdots\oplus\bar{\mathfrak{A}}_r$, 这里的 $\bar{\mathfrak{A}}_i$ 是一个理想,在看作代数时同构于域 $\Phi[x]/(p_i(x))$.

3. 代数 $\mathfrak{A}/\Phi$ 在以下意义下称为**代数的**,如果 $\mathfrak{A}$ 的每个元都是代数元. 证明: 若

$\mathfrak{A}$ 是一个整区,则 $\mathfrak{A}$ 是一个可除环.

3. 向量空间的张量积 设 $\mathfrak{M}, \mathfrak{N}, \mathfrak{P}$ 是同一域 Φ 上的向量空间,则 $\mathfrak{M}$, $\mathfrak{N}$ 到 $\mathfrak{P}$ 内的一个双线性映射指的是由积集 $\mathfrak{M} \times \mathfrak{N}$ 到 $\mathfrak{P}$ 内的映射, 它满足以下条件: 若 $x \times y$ 表示对 (x, y) $(x \in \mathfrak{M}, y \in \mathfrak{N})$ 的象,则

$$(6) \qquad \begin{aligned} (x_1 + x_2) \times y &= x_1 \times y + x_2 \times y, \\ x \times (y_1 + y_2) &= x \times y_1 + x \times y_2, \\ \alpha(x \times y) &= \alpha x \times y = x \times \alpha y \quad (\alpha \in \Phi). \end{aligned}$$

显然任何代数 $\mathfrak{A}$ 中的乘积 xy 都是 $\mathfrak{A}, \mathfrak{A}$ 到 $\mathfrak{A}$ 的双线性映射. 我们将称一个向量空间 $\mathfrak{P}$ 及 $\mathfrak{M}, \mathfrak{N}$ 到 $\mathfrak{P}$ 内的一个双线性映射$\otimes$为 $\mathfrak{M}$ 和 $\mathfrak{N}$ 的一个张量积,记为 $\mathfrak{P} = \mathfrak{M} \times \mathfrak{N}$, 如果 $(\otimes, \mathfrak{P})$ 对于双线性映射是"普遍的" (*universal*), 即满足下列条件:

若 $\mathfrak{P}'$ 是任一向量空间, 而 $\times'$ 是 $\mathfrak{M}, \mathfrak{N}$ 到 $\mathfrak{P}'$ 内的一个双线性映射, 则存在 $\mathfrak{P}$ 到 $\mathfrak{P}'$ 内的唯一的线性映射 π 使 $(x \otimes y)\pi = x \times' y$.

这个概念是环 $\mathfrak{A}$ 上的右模 $\mathfrak{M}$ 及 $\mathfrak{A}$ 上的左模 $\mathfrak{N}$ 的张量积的一般概念的特例. 对于向量空间的这种特殊情况, 我们在卷 2 的第七章中已经给出了,虽然处理方式稍有差别,但假设却完全是等价的. 特别地, 向量空间张量积存在性的证明以及我们所需要的一切基本性质几乎都已在卷 2 中给出了, 在这里我们将对其中某些基本结果给予另外的推导, 使它更能保持模的现代标准处理方法的特点.

我们首先给出张量积的一个作法, 为此我们可从一向量空间 $\mathfrak{F}$ 开始,它以对 (x, y) $(x \in \mathfrak{M}, y \in \mathfrak{N})$ 的积集 $\mathfrak{M} \times \mathfrak{N}$ 作为基, 因此 $\mathfrak{F}$ 的元可表为:

$$\xi_1(x_1, y_1) + \xi_2(x_2, y_2) + \cdots + \xi_m(x_m, y_m),$$

这里的 $\xi_i \in \Phi$, $x_i \in \mathfrak{M}$, $y_i \in \mathfrak{N}$, 而且各个对 (x_i, y_i) 都是互异的. 给定两个元后我们可以用补 0 系数的方法引入一些项、而将两元写成 $\sum_1^m \xi_i(x_i, y_i)$ 及 $\sum_1^m \eta_i(x_i, y_i)$, 则两者相等当且仅当

$\xi_i = \eta_i (i = 1, 2, \cdots, m)$;加法定义为

$$\sum_1^m \xi_i(x_i, y_i) + \sum_1^m \eta_i(x_i, y_i) = \sum_1^m (\xi_i + \eta_i)(x_i, y_i);$$

用 Φ 中 α 相乘的乘法定义为

$$\alpha\sum\xi_i(x_i, y_i) = \sum(\alpha\xi_i)(x_i, y_i).$$

立即可见 $\mathfrak{F}$ 是 Φ 上的一个向量空间. 由于 $\mathfrak{M} \times \mathfrak{N}$ 通常是无限的,因此 $\mathfrak{F}$ 通常是一个无限维空间. 现设 $\mathfrak{R}$ 是 $\mathfrak{F}$ 中由下列形式的全体向量生成的子空间:

$$\begin{aligned}&(x_1 + x_2, y) - (x_1, y) - (x_2, y)\\ &(x, y_1 + y_2) - (x, y_1) - (x, y_2)\\ &(\alpha x, y) - (x, \alpha y)\\ &\alpha(x, y) - (\alpha x, y),\end{aligned} \tag{7}$$

$x \in \mathfrak{M}$, $y \in \mathfrak{N}$, $\alpha \in \Phi$. 设 $\mathfrak{P}$ 是商空间 $\mathfrak{F}/\mathfrak{R}$,集 $x\otimes y \equiv (x, y) + \mathfrak{R}$ 是 (x, y) 在 $\mathfrak{F}/\mathfrak{R}$ 中的陪集,则有

$$\begin{aligned}&(x_1 + x_2)\otimes y - x_1\otimes y - x_2\otimes y\\ &\quad = (x_1 + x_2, y) - (x_1, y) - (x_2, y) + \mathfrak{R} = \mathfrak{R},\\ &x\otimes(y_1 + y_2) - x\otimes y_1 - x\otimes y_2\\ &\quad = (x, y_1 + y_2) - (x, y_1) - (x, y_2) + \mathfrak{R} = \mathfrak{R},\\ &\alpha(x\otimes y) - \alpha x\otimes y = \alpha(x, y) - (\alpha x, y) + \mathfrak{R} = \mathfrak{R},\\ &\alpha x\otimes y - x\otimes\alpha y = (\alpha x, y) - (x, \alpha y) + \mathfrak{R} = \mathfrak{R}.\end{aligned}$$

因此 $x \otimes y$ 是双线性的. 由于向量 (x, y) 生成 $\mathfrak{F}$, 所以陪集 $x\otimes y$ 生成 $\mathfrak{P} = \mathfrak{F}/\mathfrak{R}$.

现设 $\times'$ 是 $\mathfrak{M}$, $\mathfrak{N}$ 到向量空间 $\mathfrak{P}'$ 内的一个双线性映射, 因为向量 (x, y) 构成 $\mathfrak{F}$ 的一个基,故存在一个 $\mathfrak{F}$ 到 $\mathfrak{P}'$ 内的线性映射 π' 使 $(x, y)\pi' = x\times' y$. 令 $\mathfrak{K}$ 为 π' 的核. 则 $((x_1 + x_2, y) - (x_1, y) - (x_2, y))\pi' = (x_1 + x_2)\times' y - x_1\times' y - x_2\times' y = 0$; 故 $(x_1 + x_2, y) - (x_1, y) - (x_2, y) \in \mathfrak{K}$. 同理, $(x, y_1 + y_2) - (x, y_1) - (x, y_2) \in \mathfrak{K}$, $(\alpha x, y) - \alpha(x, y) \in \mathfrak{K}$ 以及 $(\alpha x, y) - (x, \alpha y) \in \mathfrak{K}$. 由此推出 $\mathfrak{R} \subseteq \mathfrak{K}$, 从而有 $\mathfrak{P} = \mathfrak{F}/\mathfrak{R}$ 到 $\mathfrak{P}'$ 内的线性映射 π 使 $(x\otimes y)\pi = ((x, y) + \mathfrak{R})\pi = x\times' y$. 由于空间 $\mathfrak{P} =$

$\mathfrak{F}/\mathfrak{R}$ 由元 $x\otimes y$ 生成，显然 π 被线性性质所唯一决定，而 $(x\otimes y)\pi = x\times' y$。这就证明了 $(\mathfrak{P}, \otimes)$ 是 $\mathfrak{M}$ 与 $\mathfrak{N}$ 的一个张量积，从而可写成 $\mathfrak{P} = \mathfrak{M}\otimes\mathfrak{N}$（若须指明基域 Φ 则可写成 $\mathfrak{M}\otimes_\Phi\mathfrak{N}$）。由定义立即可见：若 $(\mathfrak{P}_1, \otimes_1)$ 及 $(\mathfrak{P}_2, \otimes_2)$ 是两个张量积，则必有 $\mathfrak{P}_1$ 到 $\mathfrak{P}_2$ 内的一个线性映射使 $x\otimes_1 y \to x\otimes_2 y$，而且有一个由 $\mathfrak{P}_2$ 到 $\mathfrak{P}_1$ 内的线性映射使 $x\otimes_2 y \to x\otimes_1 y$。 因为 $x\otimes_i y$ 生成 $\mathfrak{P}_i$，这两个线性映射的两种顺序的积均为单位映射。由此推得这两个映射都是满射的(映上的)线性同构。在此意义下张量积是唯一确定的，这样我们才能说 $\mathfrak{M}$ 与 $\mathfrak{N}$ 的张量积.

设 $\{e_\alpha\}$ 及 $\{f_\beta\}$ 分别是 $\mathfrak{M}$ 和 $\mathfrak{N}$ 的生成元集，则任何 $x\in\mathfrak{M}$ 有形式 $x = \sum_1^m \xi_i e_i$，这里 $\{e_i\}$ 是 $\{e_\alpha\}$ 的一个有限子集；同理任何 $y\in\mathfrak{N}$ 有形式 $y = \sum_1^n \eta_j f_j$，而且 $\{f_j\}\subseteq\{f_\beta\}$。由 $\otimes$ 的双线性，我们有 $x\otimes y = \sum \xi_i\eta_j e_i\otimes f_j$。因为元 $x\otimes y$ 生成 $\mathfrak{M}\otimes\mathfrak{N}$，所以积 $e_\alpha\otimes f_\beta$ 生成 $\mathfrak{M}\otimes\mathfrak{N}$。 现设 $\{e_\alpha\}$ 及 $\{f_\beta\}$ 是无关的而且都是生成元集，即它们构成各自空间的一个基，我们可断言积集 $\{e_\alpha\otimes f_\beta\}$ 是 $\mathfrak{M}\otimes\mathfrak{N}$ 的一个基：由于它们是生成元，所以我们仅须证明它们是线性无关的就行了；为此可作一向量空间 $\mathfrak{P}'$，使它的基 $g_{\alpha\beta}$ 与 α 及 β 的指数集的积集 (α, β) 成 1-1 对应。若 $x=\sum\xi_i e_i$，$y=\sum\eta_j f_j$，则定义 $x\times' y = \sum\xi_i\eta_j g_{ij}$。容易验证积 $\times'$ 是双线性的，所以我们有 $\mathfrak{M}\otimes\mathfrak{N}$ 到 $\mathfrak{P}'$ 内的使 $x\otimes y\to x\times' y$ 的线性映射 π。特别地，$e_\alpha\otimes f_\beta\to e_\alpha\times' f_\beta = g_{\alpha\beta}$。由于 $g_{\alpha\beta}$ 线性无关，$e_\alpha\otimes f_\beta$ 也线性无关。这就证明了下述结论：

IX 设 $\{e_\alpha\}$ 及 $\{f_\beta\}$ 分别是 Φ 上的 $\mathfrak{M}$ 及 $\mathfrak{N}$ 的生成元集，则集 $\{e_\alpha\otimes f_\beta\}$ 生成 $\mathfrak{M}\otimes\mathfrak{N}$；更有，若 $\{e_\alpha\}$ 及 $\{f_\beta\}$ 都是基，则 $\{e_\alpha\otimes f_\beta\}$ 也是基.

第二个性质在 $\mathfrak{M}$ 和 $\mathfrak{N}$ 的双线性映射间真实地刻划了张量积。讲得更明显些： 设 $\times'$ 是从 $\mathfrak{M}$ 和 $\mathfrak{N}$ 到空间 $\mathfrak{P}'$ 的一个双线性映射，且设存在 Φ 上的 $\mathfrak{M}$ 的一个基 (e_α) 及 Φ 上的 $\mathfrak{N}$ 的一个基 (f_β)，

使得 $(e_\alpha\times'f_\beta)$ 是 $\mathfrak{P}$ 的一个基，则 $(\mathfrak{P}',\times')$ 是一个张量积，因为我们有 $\mathfrak{M}\otimes\mathfrak{N}$ 到 $\mathfrak{P}'$ 内的线性映射将 $e_\alpha\otimes f_\beta$ 映入到 $e_\alpha\times'f_\beta$. 由于 $e_\alpha\times'f_\beta$ 生成 $\mathfrak{P}'$，故此映射是满射的. 又因为 $e_\alpha\times'f_\beta$ 是线性无关的，故映射是 1—1 的. 因此我们得到一个 $\mathfrak{M}\otimes\mathfrak{N}$ 到 $\mathfrak{P}'$ 上的线性同构将 $x\otimes y$ 映到 $x\times'y$，这就推得 $(\mathfrak{P}',\times')$ 是一个张量积.

在有限维空间的场合我们有下述简单判定法:

X 令 $\times'$ 是有限维空间 $\mathfrak{M}$ 及 $\mathfrak{N}$ 到 $\mathfrak{P}'$ 内的一个双线性映射，假设 $\mathfrak{P}'$ 是由各乘积 $x\times'y$ 生成的，则维数 $[\mathfrak{P}':\Phi]\leqslant[\mathfrak{M}:\Phi]\times[\mathfrak{N}:\Phi]$，式中等式成立当且仅当 $(\mathfrak{P}',\times')$ 是 $\mathfrak{M}$ 和 $\mathfrak{N}$ 的一个张量积.

证　令 (e_i)，(f_j) 分别是 $\mathfrak{M}$ 和 $\mathfrak{N}$ 的基，则每个 $x\times'y$ 都是元素 $e_i\times f_j$ 的一个线性组合，从而 $\mathfrak{P}'$ 的两个元都是这些元的一个线性组合，由此得 $[\mathfrak{P}':\Phi]\leqslant[\mathfrak{M}:\Phi][\mathfrak{N}:\Phi]$. 此外，$(\mathfrak{P}',\times')$ 是张量积当且仅当集 $(e_i\times f_j)$ 是一个基，而这就是维数关系中等式成立的充要条件.

我们知道，若 A 是 $\mathfrak{M}$ 到 $\mathfrak{M}_1$ 内的线性映射而 B 是 $\mathfrak{N}$ 到 $\mathfrak{N}_1$ 内的线性映射，则存在一个唯一确定的由 $\mathfrak{M}\otimes\mathfrak{N}$ 到 $\mathfrak{M}_1\otimes\mathfrak{N}_1$ 内的线性映射 $A\otimes B$ 使 $(x\otimes y)(A\otimes B)=xA\otimes yB$（卷 2 的中译本 p.189). 还有，若 P 是域 Φ 的一个扩域(从而 P 是 Φ 上的一个向量空间)，$\mathfrak{M}$ 是 Φ 上的任一向量空间，则 $\mathrm{P}\otimes_\Phi\mathfrak{M}$ 可利用乘积 $\rho(\sum\rho_i\otimes x_i)=\sum\rho\rho_i\otimes x_i(\rho,\rho_i\in\mathrm{P},x_i\in\mathfrak{M})$ 看成 P 上的一个向量空间(卷 2 的中译本 p.197). 我们把这个向量空间记为 $\mathfrak{M}_\mathrm{P}$ 并称它为从 $\mathfrak{M}$ 将基域扩张到 P 所得到的空间. 若 A 是 Φ 上 $\mathfrak{M}$ 的一个线性变换，则 $1\otimes A$（它定义为 $(\sum\rho_i\otimes x_i)(1\otimes A)=\sum\rho_i\otimes x_iA$）是 P 上 $\mathfrak{M}_\mathrm{P}$ 的一个线性变换，它可看成 A 在 $\mathfrak{M}_\mathrm{P}$ 上的扩张，我们仍用同一字母 A 表示这个扩张. 若 (e_α) 是 Φ 上 $\mathfrak{M}$ 的一个基，则 $(1\otimes e_\alpha)$ 是 P 上 $\mathfrak{M}_\mathrm{P}$ 的一个基，因此 Φ 上的 $\mathfrak{M}$ 和 P 上的 $\mathfrak{M}_\mathrm{P}$ 有相同的维数. 若 $\mathfrak{M}$ 是有限维的，其基为 $(e_i)(1\leqslant i\leqslant n)$，而 A 是线性变换，它关于这个基的矩阵为 (α_{ij})，则 $e_iA=\sum\alpha_{ij}e_j$ 且 $(1\otimes e_i)A$

$=\sum \alpha_{ij}(1\otimes e_i)$。因此扩张 A 关于基 $(1\otimes e_i)$ 有同一矩阵。

我们还知道，张量积在以下意义下是交换的：存在 $\mathfrak{M}\otimes\mathfrak{N}$ 到 $\mathfrak{N}\otimes\mathfrak{M}$ 上的一个 1-1 的线性变换使得：$x\otimes y\rightarrow y\otimes x$。此外，在以下意义下结合性成立：存在一个 $(\mathfrak{M}\otimes\mathfrak{N})\otimes\mathfrak{S}$ 到 $\mathfrak{M}\otimes(\mathfrak{N}\otimes\mathfrak{S})$ 上的线性同构将 $(x\otimes y)\otimes z$ 映到 $x\otimes(y\otimes z)$ 内去。这些结果早在卷 2 的中译本 pp. 187—188 中已建立。我们将在下列几个习题中指出另外的证法。

习　题　2

1. 证明：若 $\{f_\beta\}$ 是 $\mathfrak{N}$ 的一个生成元集，则 $\mathfrak{M}\otimes\mathfrak{N}$ 的每个元有形式 $\sum x_i\otimes f_i$，这里 $\{f_i\}$ 是 $\{f_\beta\}$ 的一个有限子集，$x_i\in\mathfrak{M}$. 证明：若 $\{f_\beta\}$ 线性无关，则 $\sum x_i\otimes f_i=0$ 当且仅当每个 $x_i=0$.

2. 证明：若 $\mathfrak{M}_1$ 是 $\mathfrak{M}$ 的一个子空间，则由所有向量 $x_1\otimes y(x_1\in\mathfrak{M}_1, y\in\mathfrak{N})$ 生成的子空间 $\mathfrak{M}_1\otimes\mathfrak{N}$ 是 $\mathfrak{M}_1$ 与 $\mathfrak{N}$ 的关于定义在 $\mathfrak{M}\otimes\mathfrak{N}$ 中的$\otimes$的张量积.

3. 令 $\mathfrak{K}$ 是 $\mathfrak{M}$ 的一个子空间，$\mathfrak{L}$ 是 $\mathfrak{N}$ 的一个子空间，证明 $(\mathfrak{M}/\mathfrak{K})\otimes(\mathfrak{N}/\mathfrak{L})$ 与 $(\mathfrak{M}\otimes\mathfrak{N})/(\mathfrak{K}\otimes\mathfrak{N}+\mathfrak{M}\otimes\mathfrak{L})$ 在一个使 $(x+\mathfrak{K})\otimes(y+\mathfrak{L})\rightarrow x\otimes y+(\mathfrak{K}\otimes\mathfrak{N}+\mathfrak{M}\otimes\mathfrak{L})$ 的线性映射下同构.

4. 设 $\mathfrak{M}_1, \mathfrak{M}_2, \cdots, \mathfrak{M}_r$ 及 $\mathfrak{P}$ 是 Φ 上的向量空间，利用下列性质规定一个 r 线性映射 $(x_1,\cdots,x_r)\rightarrow x_1\times x_2\times\cdots\times x_r\in\mathfrak{P}(x_i\in\mathfrak{M}_i)$：

$$x_1\times\cdots\times(x_i'+x_i'')\times\cdots\times x_r=x_1\times\cdots\times x_i'\times\cdots\times x_r$$
$$+x_1\times\cdots\times x_i''\times\cdots\times x_r,$$
$$\alpha(x_1\times\cdots\times x_r)=x_1\times\cdots\times\alpha x_i\times\cdots\times x_r.$$

证明：存在一个 $\mathfrak{P}$ 及一个 $\mathfrak{M}_1,\cdots,\mathfrak{M}_r$ 到 $\mathfrak{P}$ 内的 r 线性映射，使得：若 $(x_1,\cdots,x_r)\rightarrow x_1\times'x_2\times'\cdots\times'x_r$ 是 $\mathfrak{M}_1,\cdots,\mathfrak{M}_r$ 到 $\mathfrak{P}'$ 内的一个 r 线性映射，则必存在唯一的一个 $\mathfrak{P}$ 到 $\mathfrak{P}'$ 内的线性映射 π 使 $(x_1\otimes\cdots\otimes x_r)\pi=x_1\times'\cdots\times'x_r$. 这个 $\mathfrak{P}$ 连同它的积表示张量积 $\mathfrak{M}_1\otimes\mathfrak{M}_2\otimes\cdots\otimes\mathfrak{M}_r$.

5. 分别利用使 $x\otimes y\otimes z\rightarrow x\otimes(y\otimes z)$ 及 $(x\otimes y)\otimes z$ 的线性映射证明：$\mathfrak{M}\otimes\mathfrak{N}\otimes\mathfrak{P}$ 同构于 $\mathfrak{M}\otimes(\mathfrak{N}\otimes\mathfrak{P})$ 及 $(\mathfrak{M}\otimes\mathfrak{N})\otimes\mathfrak{P}$、并推广到 r 个因子的情形上去.

6. 证明：在线性映射 $x\otimes y\rightarrow y\otimes x$ 下，$\mathfrak{M}\otimes\mathfrak{N}$ 同构于 $\mathfrak{N}\otimes\mathfrak{M}$.（提示：给定 $\mathfrak{N}\otimes\mathfrak{M}$ 后，定义 $x\times'y=y\otimes x$，$x\in\mathfrak{M}$，$y\in\mathfrak{N}$. 证明这样就给出了一个 $\mathfrak{M}$, $\mathfrak{N}$ 到 $\mathfrak{N}\otimes\mathfrak{M}$ 内的双线性映射，再应用 $\mathfrak{M}\otimes\mathfrak{N}$ 的定义性质；然后颠倒 $\mathfrak{M}$ 与 $\mathfrak{N}$ 的位置）.

4. 代数的张量积　我们知道，若 $\mathfrak{A}_1$ 和 $\mathfrak{A}_2$ 是 Φ 上的两个代数，则向量空间 $\mathfrak{A}=\mathfrak{A}_1\otimes\mathfrak{A}_2$ 关于它的向量空间的合成及下列乘法构成一个代数：

(8) $$\left(\sum_i a_{1i}\otimes a_{2i}\right)\left(\sum_j b_{1j}\otimes b_{2j}\right)=\sum_{i,j} a_{1i}b_{1j}\otimes a_{2i}b_{2j},$$

其中，$a_{1i}, b_{1j}\in\mathfrak{A}_1$, $a_{2i}, b_{2j}\in\mathfrak{A}_2$（卷 2 的中译本 p.201）．由 $\mathfrak{A}_1$ 和 $\mathfrak{A}_2$ 的结合性推得 $\mathfrak{A}_1\otimes\mathfrak{A}_2$ 也是可结合的．若 1_i 是 $\mathfrak{A}_i$ 的单位元，则 $1_1\otimes 1_2$ 也是 $\mathfrak{A}=\mathfrak{A}_1\otimes\mathfrak{A}_2$ 的单位元 1．而且若 $\mathfrak{A}_i$ 是交换的，则 $\mathfrak{A}$ 也是交换的．代数张量积的基本性质是以下的同态定理：

XI 设 $\mathfrak{A}_i(i=1,2)$ 是 Φ 上的两个代数，S_i 是 $\mathfrak{A}_i$ 到代数 $\mathfrak{B}$ 内的同态，它们使 $a_1^{s_1}a_2^{s_2}=a_2^{s_2}a_1^{s_1}(a_1\in\mathfrak{A}_1,\ a_2\in\mathfrak{A}_2)$，则存在一个 $\mathfrak{A}=\mathfrak{A}_1\otimes\mathfrak{A}_2$ 到 $\mathfrak{B}$ 内的同态 s，使得

(9) $$\left(\sum a_{1i}\otimes a_{2i}\right)^s=\sum a_{1i}^{s_1}a_{2i}^{s_2}.$$

证　代数积 $a_1\times' a_2\equiv a_1^{s_1}a_2^{s_2}\in\mathfrak{B}$ 可以定义一个 $\mathfrak{A}_1, \mathfrak{A}_2$，到 $\mathfrak{B}$ 内的双线性映射，这由 s_i 的线性性质及 $\mathfrak{B}$ 的乘法合成的性质是很容易看出来的．由这定义推得：有一个 $\mathfrak{A}_1\otimes\mathfrak{A}_2$ 到 $\mathfrak{B}$ 内的线性映射 s 使 $(a_1\otimes a_2)^s=a_1^{s_1}a_2^{s_2}$，故 s 有形式(9)．我们有 $((a_1\otimes a_2)(b_1\otimes b_2))^s=(a_1b_1\otimes a_2b_2)^s=(a_1b_1)^{s_1}(a_2b_2)^{s_2}=a_1^{s_1}b_1^{s_1}a_2^{s_2}b_2^{s_2}=a_1^{s_1}a_2^{s_2}b_1^{s_1}b_2^{s_2}=((a_1\otimes a_2)^s(b_1\otimes b_2)^s)$．这就是说 s 是一个代数同态．

假设下列条件在 $\mathfrak{B}$ 中成立：

(i) 若 (e_α) 是 Φ 上 $\mathfrak{A}_1$ 的一个基，而 (f_β) 是 Φ 上 $\mathfrak{A}_2$ 的一个基，则集 $\{e_\alpha^{s_1}f_\beta^{s_2}\}$ 必线性无关．

有时我们使用以下等价条件更为方便：

(i′) 若 (f_β) 是 Φ 上 $\mathfrak{A}_2$ 的一个基，则由关系

$$a_1^{s_1}f_1^{s_2}+a_2^{s_1}f_2^{s_2}+\cdots+a_m^{s_1}f_m^{s_2}=0\quad(a_i\in\mathfrak{A}_1,\ f_i\in\{f_\beta\})$$

可推得每个 $a_i=0$（参看 §3 习题的第 1 题）．

我们已经看到，若 (i) 或 (i)′ 成立，则由(9)给出的映射 s 可看作向量空间的 $\mathfrak{A}=\mathfrak{A}_1\otimes\mathfrak{A}_2$ 到 $\mathfrak{B}$ 内的一个同构． 因为这是一个代数同态，显然它也是一个代数同构．我们要附带指出：(i) 不成立，除非 s_1 与 s_2 都是同构．

我们所得到的结果实际上给出了 $\mathfrak{A}_1\otimes\mathfrak{A}_2$ 的一个内部特征．为此请注意 $a_1\to a_1^{s_1}\equiv a_1\otimes 1_2$ 及 $a_2\to a_2^{s_2}\equiv 1_1\otimes a_2$，它们分别是 $\mathfrak{A}_1$ 及 $\mathfrak{A}_2$ 到 $\mathfrak{A}_1\otimes\mathfrak{A}_2$ 内的同态，这两个映射的线性性质由 $a_1\otimes a_2$ 的

双线性性质可以得到,而对于乘法的同态则由(9)立即可得到. 至于可交换性这个条件: $a_1^{s_1}a_2^{s_2} = a_2^{s_2}a_1^{s_1}$ 也是很明显的,因为 $a_1^{s_1}a_2^{s_2} = (a_1\otimes 1_2)(1_1\otimes a_2) = a_1\otimes a_2 = (1_1\otimes a_2)(a_1\otimes 1_2) = a_2^{s_2}a_1^{s_1}$. 最后, 若 (e_α) 及 (f_β) 分别是 $\mathfrak{A}_1$ 及 $\mathfrak{A}_2$ 的基, 则集 $\{e_\alpha^{s_1}f_\beta^{s_2}\} = \{e_\alpha\otimes f_\beta\}$ 必线性无关. 于是 $(e_\alpha^{s_1})$ 是 $\mathfrak{A}_1^{s_1} = \{a_1\otimes 1\}$ 的一个基而 $(f_\beta^{s_2})$ 是 $\mathfrak{A}_2^{s_2}$ 的一个基. 还因为 s_1 及 s_2 都是同构,我们可将 $\mathfrak{A}_1^{s_1}$ 与 $\mathfrak{A}_1$, $\mathfrak{A}_2^{s_2}$ 与 $\mathfrak{A}_2$ 等同起来.以上结果导出张量积的以下内部特征:

XII 设 $\mathfrak{A}$ 是一个代数, $\mathfrak{A}_1$, $\mathfrak{A}_2$ 是满足下列三个条件的子代数:

(i) $a_1a_2 = a_2a_1$, $a_i \in \mathfrak{A}_i$.

(ii) 若 (e_α) 是 $\mathfrak{A}_1$ 的一个基, (f_β) 是 $\mathfrak{A}_2$ 的一个基, 则$\{e_\alpha f_\beta\}$ 是一个线性无关集.

(iii) $\mathfrak{A}$ 由 $\mathfrak{A}_1$ 及 $\mathfrak{A}_2$ 生成.

则 $\Sigma a_{1i}\otimes a_{2i} \to \sum a_{1i}a_{2i}$ 是 $\mathfrak{A}_1\otimes\mathfrak{A}_2$ 到 $\mathfrak{A}$ 上的一个同构.

由这个结果及 $\mathfrak{A}_1\otimes\mathfrak{A}_2$ 本身所看到的情况,我们可以得到: 如果上述条件 (i) — (iii) 被满足, 我们就可以称 $\mathfrak{A}$ 是它的子代数 $\mathfrak{A}_1$ 及 $\mathfrak{A}_2$ 的张量积. 如我们已经看到的,条件 (ii) 还可换成以下等价条件:

(ii)′ 若 (f_β) 是 $\mathfrak{A}_2$ 的一个基, 则由

$$a_1f_1 + a_2f_2 + \cdots + a_mf_m = 0 \quad (a_i \in \mathfrak{A}_1,\ f_i \in (f_\beta))$$

可推出每个 $a_i = 0$.

当然, $\mathfrak{A}_1$ 与 $\mathfrak{A}_2$ 的位置可以对调,我们还可进一步将 (ii), (iii) 合并为以下的单独条件: 若 (e_α) 是 $\mathfrak{A}_1$ 的一个基而 (f_β) 是 $\mathfrak{A}_2$ 的一个基, 则 $(e_\alpha f_\beta)$ 是 $\mathfrak{A}$ 的一个基.特别地,对于有限维代数,这等价于维数条件: $[\mathfrak{A}:\Phi] = [\mathfrak{A}_1\mathfrak{A}_2:\Phi] = [\mathfrak{A}_1:\Phi][\mathfrak{A}_2:\Phi]$(参考 X).

习 题 3

1. 设 $\mathfrak{A}$ 是域 Φ 上的代数, $\mathfrak{A}[x]$ 是 $\mathfrak{A}$ 上一个未定元 x 的多项式代数,证明: $\mathfrak{A}[x]$ 是子代数 $\mathfrak{A}$ (由 $\mathfrak{A}[x]$ 中的常数构成) 与 x 的系数在 Φ 中的多项式子代数 $\Phi[x]$ 的张量积. 利用这个结果证明: $\Phi[x, y]$ (x, y 都是未定元) 是它的子代数 $\Phi[x]$ 与 $\Phi[y]$ 的张量积.

2.设 $\Phi(x, y)$ 是未定元 x, y 的有理分式域（即 $\Phi[x, y]$ 的分式域），$\mathfrak{A}$ 是分母形如 $f(x)g(y)$ 的分式组成的子集，这里的 $f(x) \in \Phi[x]$，$g(y) \in \Phi[y]$. 证明：$\mathfrak{A}$ 是 $\Phi(x, y)$ 的一个子代数，它包含子代数 $\Phi(x)$，$\Phi(y)$，后两者分别是 $\Phi[x]$ 与 $\Phi[y]$ 的分式域. 证明 $\mathfrak{A}$ 是这些子代数的张量积而 $\mathfrak{A}$ 不是一个域.

第一章

有限维扩张域

若Φ是域P的子域，则我们知道可把P看作Φ上的代数，本章将主要考虑P是子域Φ上的有限维扩张的情况．我们将特别关心伽罗瓦理论的那些一般结果，它在整个代数学，特别是在代数数论中是极为重要的．我们将考虑正规性，可分性，扩张域的纯不可分性，伽罗瓦上同调，正则表示，迹与范数等概念．有限域的基本结果将被推出，两个扩张域的合成的概念亦将被考虑．

在本书的大部分问题的考虑中，实际上是在全书中，我们经常给定一个域Φ，而后考虑扩张域P/Φ．得到此种扩张域的方法我们早在卷1中(中译本的 p.96—97)就指出过了．但在本章开始时我们将采用不同的观点，我们给出的是顶域P (topfield P) 而要往下看它的各种子域；我们不要求这些子域包含任何特殊的子域(素域当然除外)．这里的处理方法是抽象的，这是说它毋需扩张域结构的任何知识．虽然如此，我们还是可以通盘考察给定域P中的所有有限余维数的子域以及在P中是伽罗瓦域的子域．这些考察由两个一般的"伽罗瓦对应"给出，经过这些颇为抽象的考虑后我们将追溯到Φ，然后再用系数在P中的多项式方程的语言将一般结果应用到扩张域P/Φ上去．

1. 与域的映射相关联的一些向量空间 设E及P是两个域，$\mathfrak{L}(E,P)$表示E的加群$(E,+)$到加群$(P,+)$内的同态的集．集$\mathfrak{L}(E,P)$关于由$\varepsilon(A+B)=\varepsilon A+\varepsilon B(\varepsilon\in E)$定义的合成$A+B$来说构成一个群．可以验证$A+B\in\mathfrak{L}(E,P)$且群条件成立：$\mathfrak{L}(E,P)$的0是使$\varepsilon 0=0$对于$E$中一切$\varepsilon$成立的映射0(等式右端的0是P的零元)，而$-A$则由$\varepsilon(-A)=-\varepsilon A$给出(参考卷1的§2.13及卷2的§2.2)．设$\Delta$是第三个域而$A\in\mathfrak{L}(E,$

P), $B \in \mathfrak{L}(\mathrm{P}, \Delta)$，则由 $\varepsilon(AB) = (\varepsilon A)B$ 定义的结果 AB 是 $\mathfrak{L}(E, \Delta)$ 的一个元，这个合成适合两个分配律，它们的联合形式是：若 $A_1, A_2 \in \mathfrak{L}(E, \mathrm{P})$，$B_1, B_2 \in \mathfrak{L}(\mathrm{P}, \Delta)$，则

$$(A_1 + A_2)(B_1 + B_2) = A_1B_1 + A_1B_2 + A_2B_1 + A_2B_2.$$

最后，乘法结合律成立：设 Γ 是另一域且 $A \in \mathfrak{L}(E, \mathrm{P})$，$B \in \mathfrak{L}(\mathrm{P}, \Delta)$，$C \in \mathfrak{L}(\Delta, \Gamma)$，则 $(AB)C = A(BC) \in \mathfrak{L}(E, \Gamma)$. 所有这些结论都可以和卷 2 的 § 2.2 中考察线性映射的合成时一样加以验证，我们把这些验证留给读者.

由以上的结果可推出 $\mathfrak{L}(E, E)$ 关于加法和乘法运算作成一个环，这恰是卷 1 的 § 2.13 所考虑的一般情况下的加群 $(E, +)$ 的自同态环. 若 $\rho \in \mathrm{P}$，则 P 内的映射 $\rho_R: \xi \to \xi\rho(=\rho\xi)$ 属于 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$，从对于 $\mathfrak{L}(E, \mathrm{P})$ 中的 A 及 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 中的 B 有 $AB \in \mathfrak{L}(E, \mathrm{P})$，可见 $A\rho_R \in \mathfrak{L}(E, \mathrm{P})$. 这种考察使我们可以将 $\mathfrak{L}(E, \mathrm{P})$ 转变成域 P 上的右向量空间，为此可对 $A \in \mathfrak{L}(E, \mathrm{P})$ 及 $\rho \in \mathrm{P}$ 规定 $A\rho = A\rho_R$，从而有

$$(A + B)\rho = (A + B)\rho_R = A\rho_R + B\rho_R = A\rho + B\rho,$$
$$A(\rho + \sigma) = A(\rho + \sigma)_R = A(\rho_R + \sigma_R)$$
$$= A\rho_R + A\sigma_R = A\rho + A\sigma,$$
$$A(\rho\sigma) = A(\rho\sigma)_R = A(\rho_R\sigma_R) = (A\rho_R)\sigma_R = (A\rho)\sigma,$$
$$A1 = A1_R = A,$$

这就证明了 $\mathfrak{L}(E, \mathrm{P})$ 是 P 上的一个右向量空间.

其次，若令 ε_R 表示 E 中的映射 $\eta \to \eta\varepsilon$，则 $\varepsilon_R \in \mathfrak{L}(E, E)$. 因此，若 $A \in \mathfrak{L}(E, \mathrm{P})$，则 $\varepsilon_R A \in \mathfrak{L}(E, \mathrm{P})$. 我们这时若定义 $\varepsilon A = \varepsilon_R A$，则又可将 $\mathfrak{L}(E, \mathrm{P})$ 看作 E 上的左向量空间. 这里必须声明的是：如果我们这样做就会在书写 εA 时产生混乱，因为 εA 既可表示 ε 在 A 下的象，又可表示自同态 $\varepsilon_R A$. 因此我们将避免把 $\mathfrak{L}(E, \mathrm{P})$ 作为 E 上的左向量空间考虑，在需要时则用乘积 $\varepsilon_R A$ 代替.

上述全部结果也可应用到给定域 Φ 上的域去. 考虑域 E/Φ 及 P/Φ，与此相联系自然可以考虑 $\mathfrak{L}(E, \mathrm{P})$ 的子集 $\mathfrak{L}_\Phi(E, \mathrm{P})$，

它由Φ上的向量空间E到Φ上的向量空间P内的所有线性变换所构成.若$\alpha\in\Phi$而$\xi,\rho\in$ P,则$(\alpha\xi)\rho_R=(\alpha\xi)\rho=\alpha(\xi P_R)$，由此得到$\rho_R\in\mathfrak{L}_\Phi(P,P)$. 若$A\in\mathfrak{L}_\Phi(E,P)$,则$A\rho=A\rho_R\in\mathfrak{L}_\Phi(E,P)$;所以$\mathfrak{L}_\Phi(E,P)$是P上的右向量空间$\mathfrak{L}(E,P)$的一个子空间.若$\mathfrak{A}$是P上的任一右向量空间,我们把它在P上的维数记作$[\mathfrak{M}:P]_R$,则可得下列关于$[\mathfrak{L}_\Phi(E,P):P]_R$的重要结果:

定理 1. 设E/Φ, P/Φ是Φ上的两个域，而$\mathfrak{L}_\Phi(E,P)$是E/Φ到P/Φ内的线性映射所构成的P上的右向量空间，则$[E:\Phi]$有限当且仅当$[\mathfrak{L}_\Phi(E,P):P]_R$有限，并且当二者都有限时,有

$$(1)\qquad [E:\Phi]=[\mathfrak{L}_\Phi(E,P):P]_R.$$

证 设$\eta_1,\eta_2,\cdots,\eta_n$是$E$的$\Phi$上的线性无关元，则可把这个集嵌入$\Phi$上的$E$的一个基$\{\eta_\alpha\}$里面去(卷 2 的中译本 p.215).现对于每个η_α选取一个对应元$\tau_\alpha\in$ P，则必存在一个唯一的元$A\in\mathfrak{L}_\Phi(E,P)$,使对于每个$\eta_\alpha$有$\eta_\alpha A=\tau_\alpha$. 由此推得：对于每个$i=1,2,\cdots,n$,存在一个线性映射$E_i$(未必唯一!)使$\eta_iE_i=1$, $\eta_jE_i=0$ (若$j\neq i$). 今若$\rho_i\in$ P,

$$\eta_j\left(\sum_1^n E_i\rho_i\right)=\sum_{i=1}^n(\eta_jE_i)\rho_i=\rho_j.$$

因此由$\sum_1^n E_i\rho_i=0$可推得每个$\rho_i=0$，这表明：若$[E:\Phi]$是无限的,则对于每个n存在$\mathfrak{L}_\Phi(E,P)$的n个右P无关元,故对于每个n有$[\mathfrak{L}_\Phi(E,P):P]_R\geqslant n$，因此维数是无限的. 其次假设$[E:\Phi]=n<\infty$，而将各$\eta$组成一个基. 令$A\in\mathfrak{L}_\Phi(E,P)$而且使$\eta_iA=\rho_i$，则$\eta_j\left(\sum_1^n E_i\rho_i\right)=\rho_j=\eta_jA$. 因此$A$和$\Sigma E_i\rho_i$对于$E/\Phi$的基$(\eta_1,\eta_2,\cdots,\eta_n)$有相同的作用,故

$$A=\sum_1^n E_i\rho_i,$$

而且由于E_i是P上的右无关元,故组成P上的$\mathfrak{L}_\Phi(E,P)$的一个

素，因此 $[\mathfrak{L}_\Phi(E, \mathrm{P}):\mathrm{P}]_R = n = [E:\Phi]$. 证毕.

我们现在丢掉 Φ，再次把 E 及 P 看作任意域，而 $\mathfrak{L}(E, \mathrm{P})$ 是 $(E, +)$ 到 $(\mathrm{P}, +)$ 内的同态群．仍象前面一样把它看成 P 上的一个右向量空间，设 $\mathfrak{A}$ 是这一空间的一个子空间，ε 是 E 的一个固定元，则 ε 可由法则 $f_\varepsilon(A) = \varepsilon A \in \mathrm{P}$ 确定一个 $\mathfrak{A}$ 到 P 内的映射 f_ε，我们有 $f_\varepsilon(A + B) = \varepsilon(A + B) = \varepsilon A + \varepsilon B = f_\varepsilon(A) + f_\varepsilon(B)$，且若 $\rho \in \mathrm{P}$，则 $f_\varepsilon(A\rho) = \varepsilon(A\rho) = (\varepsilon A)\rho = f_\varepsilon(A)\rho$. 因此 f_ε 是 P 上的右向量空间 $\mathfrak{A}$ 到 P 上的一维空间 P 内的一个 P 线性映射，即 $f_\varepsilon \in \mathfrak{A}^*$，这里 $\mathfrak{A}^*$ 是 $\mathfrak{A}$ 的共轭空间，当然 $\mathfrak{A}^*$ 是 P 上的一个左向量空间．上述过程中产生一个线性函数集 $\{f_\varepsilon | \varepsilon \in E\}$，这个集在以下意义下是"完全的"：若对于所有的 ε 都有 $f_\varepsilon(A) = 0$，则 $A = 0$. 这是显然的，因为要求："对于所有 ε 都有 $\varepsilon A = 0$" 恰是 $A = 0$ 的定义．对此可证以下有用的结论

引理. 设 $\mathfrak{A}$ 是 P 上 $\mathfrak{L}(E, \mathrm{P})$ 的一个子空间使得 $[\mathfrak{A}:\mathrm{P}]_R = n < \infty$，则存在元 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n \in E$ 及 P 上 $\mathfrak{A}$ 的一个右基 $E_1, E_2, \cdots, E_n$ 使 $\varepsilon_i E_j = \delta_{ij}$（若 $i \neq j$，则 $\delta_{ij} = 0; \delta_{ii} = 1$）.

证　已知 $[\mathfrak{A}:\mathrm{P}]_R = n < \infty$，则可推得共轭空间 $\mathfrak{A}^*$ 是 n 维的．令 $\mathfrak{B}^*$ 是 $\mathfrak{A}^*$ 的由线性函数 $f_\varepsilon(\varepsilon \in E)$ 生成的子空间．因为由 $f(A) = 0$ 对一切 $f \in \mathfrak{B}^*$ 成立可推出 $A = 0$，所以有 $\mathfrak{B}^* = \mathfrak{A}^*$（卷 2，§ 2.10），故可找得 n 个线性函数 $f_{\varepsilon_1}, f_{\varepsilon_2}, \cdots, f_{\varepsilon_n}$，它们形成 $\mathfrak{A}^*$ 的一个基．由于 $\mathfrak{A}$ 可看成 $\mathfrak{A}^*$ 的共轭空间，我们可找得 P 上 $\mathfrak{A}$ 的一个基 $E_1, E_2, \cdots, E_n$ 使 $f_{\varepsilon_i}(E_j) = \delta_{ij}$，由 f_ε 的意义即可得到要求证的 $\varepsilon_i E_j = \delta_{ij}$.

2. 贾柯勃逊-布尔巴基（Jacobson-Bourbaki）对应　设 P 是一个域，$\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 是加群 $(\mathrm{P}, +)$ 的自同态环，和前面一样，我们把 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 看作 P 上的右向量空间．若 Φ 是一个子域，则 P/Φ 的线性变换环 $\mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P})$ 是 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 的一个子环，同时也是 P 上的 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 的一个子空间．而且，在定理 1 中我们还看到：若 Φ 在 P 中是有限余维数的，即 $[\mathrm{P}:\Phi] = n < \infty$，则 $[\mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P}):\mathrm{P}]_R = n$. $\mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P})$ 的这些性质根本与子域 Φ 无关，我们现在来证

明它们是集 $\mathfrak{L}_\Phi(P, P)$ 的特征，这是下列定理的直接结果：

定理 2 （贾柯勃逊-布尔巴基）. 设 P 是一个域而 $\mathfrak{A}$ 是$(P, +)$的自同态集，满足

(i) $\mathfrak{A}$ 是 $(P, +)$ 的自同态环 $\mathfrak{L}(P, P)$ 的一个子环(在导言 p.4 中我们已约定，它包含恒等映射).

(ii) $\mathfrak{A}$ 是 $\mathfrak{L}(P, P)$ 作为 P 上右向量空间的一个子空间.

(iii) $[\mathfrak{A}:P]_R = n < \infty$.

令 Φ 为 P 的元 α 的子集，它们对于所有的 $A \in \mathfrak{A}$ 都有 $\alpha_R A = A\alpha_R$，则 Φ 是 P 的一个子域，$[P:\Phi] = n$，而且 $\mathfrak{A} = \mathfrak{L}_\Phi(P, P)$ 是 P/Φ 的线性变换的完全集.

证 （霍赫希尔德 Hochschild）Φ 是子域的验证是容易的，我们略去了. 应用 § 1 的引理可得到 P 中的元 $\rho_1, \rho_2, \cdots, \rho_n$ 及 P 上 $\mathfrak{A}$ 的一个右基 $(E_1, E_2, \cdots, E_n)$ 使 $\rho_i E_j = \delta_{ij}$. 因为 $\rho_R \sigma_R = \sigma_R \rho_R$ 对于 P 中的任何元 ρ, σ 都成立，故 Φ 是 P 中满足 $\alpha_R E_i = E_i \alpha_R (i = 1, 2, \cdots, n)$ 的元 α 的集. 由 $\rho_i E_j = \delta_{ij}$ 还可推出：若将 $\mathfrak{A}$ 中的元 A 表成 $A = \sum_1^n E_i \sigma_i$，则 $\rho_j A = \sum_i (\rho_j E_i)\sigma_i = \sigma_j$，因此任何 A 用基表示时均可写成：

$$A = \sum_1^n E_i(\rho_i A) \quad 或 \quad A = \sum_1^n E_i(\rho_i A)_R.$$

我们将利用这个公式来证明每个 E_i 将 P 映入 Φ 内. 为此令 σ 为 P 的任意元，考虑映射 $E_j \sigma_R E_k (j, k = 1, 2, \cdots, n)$，由于 $\mathfrak{A}$ 是自同态环的一个子环，所以它属于 $\mathfrak{A}$. 将所得公式应用于 $A = E_j \sigma_R E_k$ 得

$$\begin{aligned} E_j \sigma_R E_k &= \sum_i E_i(\rho_i E_j \sigma_R E_k)_R \\ &= E_j(1\sigma_R E_k)_R \\ &= E_j(\sigma E_k)_R. \end{aligned}$$

这意味着：对于 P 中的任意元 ρ 我们总有：

$$\rho E_j \sigma_R E_k = \rho E_j (\sigma E_k)_R,$$

即

$$((\rho E_i)\sigma)E_k = (\rho E_i)(\sigma E_k),$$

因此

$$(\sigma(\rho E_i))E_k = (\sigma E_k)(\rho E_i).$$

若将 σ 看作变项，此式给出算子恒等式 $(\rho E_i)_R E_k = E_k(\rho E_i)_R$，由它可推出 $\rho E_i \in \Phi$，并且这对于一切 $\rho \in$ P 都成立，现在我们能够证明最初给出的 ρ_i 作成 P/Φ 的一个基：设 $\sigma \in$ P，在 P 中考察元 $\sigma' = \sigma - \sum_j (\sigma E_j)\rho_j$，因为 $\sigma E_j \in \Phi$ 而且对于 Φ 中的 α，$\alpha_R E_k = E_k \alpha_R$，我们有

$$\sigma' E_k = \sigma E_k - \left(\sum_j (\sigma E_j)\rho_j\right) E_k = \sigma E_k - \left(\sum_j \rho_j (\sigma E_j)_R\right) E_k$$

$$= \sigma E_k - \sum_j (\rho_j E_k)(\sigma E_j)_R = \sigma E_k - \sigma E_k = 0,$$

由于 $1 \in \mathfrak{A}$，对于适当选取的 $\lambda_k \in$ P 有 $1 = \Sigma E_k \lambda_k$. 因此由 $\sigma' E_k = 0$ 可推出 $\sigma' 1 = 0$，故 $\sigma' = 0$. 由此可见 $\sigma = \Sigma(\sigma E_j)\rho_j$ 是 ρ_j 的一个 Φ 线性组合。若 $\Sigma \alpha_i \rho_i = 0$，$\alpha_i \in \Phi$，则

$$\alpha_j = (\Sigma \alpha_i \rho_i)E_j = 0,$$

所以 $(\rho_1, \rho_2, \cdots, \rho_n)$ 是 Φ 上的 P 的一个基而 $[\mathrm{P}:\Phi] = n$. 由于 $\alpha_R A = A\alpha_R$ 对每个 $\alpha \in \Phi$ 及 $A \in \mathfrak{A}$ 成立，而每个 $A \in \mathfrak{A}$ 都是 Φ 上 P 的一个线性变换，因此 $\mathfrak{A} \leqslant \mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P})$. 但由定理 1 可知 $[\mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P}):\mathrm{P}]_R = n$，又 $[\mathfrak{A}:\mathrm{P}]_R = n$，故 $\mathfrak{A} = \mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P})$.

定理 2 使我们能够为一个域 P 建立第一个最一般的"伽罗瓦对应"，这关系到两个对象的类，一个是 P 中有限余维数子域 Φ 的类 $\mathscr{F}$，另一个是 (P, +) 的具有本定理性质 (i), (ii), (iii) 的自同态集的类 $\mathscr{R}$，对每个 $\Phi \in \mathscr{F}$ 我们令 $R(\Phi) = \mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P})$ 与之对应，这是 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 的一个子环，也是 P 上 $\mathfrak{L}(\mathrm{P}, \mathrm{P})$ 的一个子空间，而且适合 $[\mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P}):\mathrm{P}]_R < \infty$，因此 $R(\Phi) = \mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P}) \in \mathscr{R}$. 另一方面，若 $\mathfrak{A} \in \mathscr{R}$，则可令子域

$$F(\mathfrak{A}) = \Phi = \{\alpha | \alpha \in \mathrm{P}, \alpha_R A = A\alpha_R, A \in \mathfrak{A}\}$$

与之对应，这是P中有限余维数的子域，因此它属于 $\mathscr{F}$. 由定理2，我们有 $R(F(\mathfrak{A}))=\mathfrak{A}$. 若 $\Phi\in\mathscr{F}$ 且 $\mathfrak{A}=R(\Phi)=\mathfrak{L}_\Phi(\mathrm{P},\mathrm{P})$，则由定理1有 $[\mathfrak{A}:\mathrm{P}]_R=[\mathrm{P}:\Phi]$；而由定理2有 $[\mathfrak{A}:\mathrm{P}]_R=[\mathrm{P}:F(\mathfrak{A})]$. 若 $\alpha\in\Phi$，我们确有 $\alpha_R A=A\alpha_R$ 对于 $A\in\mathfrak{A}$ 成立. 因此由 F 的定义，$\Phi\leqslant F(\mathfrak{A})$. 因为

$$[\mathrm{P}:\Phi]=[\mathrm{P}:F(\mathfrak{A})][F(\mathfrak{A}):\Phi]$$

(导言的 VI) 及 $[\mathrm{P}:\Phi]=[\mathrm{P}:F(\mathfrak{A})]$，我们有 $[F(\mathfrak{A}):\Phi]=1$；于是 $\Phi=F(\mathfrak{A})=F(R(\Phi))$. 上述的两个关系

$$R(F(\mathfrak{A}))=\mathfrak{A},\quad \mathfrak{A}\in\mathscr{R},$$

$$F(R(\Phi))=\Phi,\quad \Phi\in\mathscr{F}$$

推出 R 及 F 分别是 $\mathscr{F}$ 到 $\mathscr{R}$ 上的及 $\mathscr{R}$ 到 $\mathscr{F}$ 上的、互逆的，1-1映射. 这里要注意的是：R 及 F 的定义表明这两个映射对于包含关系是反序的：若子域 $\Phi_1\subseteq\Phi_2$ 则 $R(\Phi_1)\supseteq R(\Phi_2)$；而对于 $\mathfrak{A}_i\in\mathscr{R}$，如果 $\mathfrak{A}_1\subseteq\mathfrak{A}_2$，则 $F(\mathfrak{A}_1)\supseteq F(\mathfrak{A}_2)$.

我们将于§4在域P的有限自同构群与P中某些有限余维数子域之间建立一个伽罗瓦对应，后面(第四章的§8)我们还将在P中的某些导子李代数与P的某些子域之间建立类似的对应. 这两种对应均可由刚才给出的一般"贾柯勃逊-布尔巴基对应"导出. 对此要附带说明的是：对于某些环 $\mathfrak{A}\in\mathscr{R}$，我们还需要特殊生成元的某些信息，例如对于自同构理论来说，这些生成元是P的自同构. 我们所需要的这方面的结果将在下一节中导出.

习 题 4

1. 设 $\mathfrak{A}$ 是 $(\mathrm{P},+)$ 的满足定理2条件 (i) 及 (ii) 的自同态集，证明 $\mathfrak{A}$ 是自同态的一个不可约环(卷2的中译本 p.233). 利用这种环的稠密性定理 (卷2的中译本 p.247)证明：若 $\rho_1,\rho_2,\cdots,\rho_m$ 是 Φ 无关元(Φ 如定理2所示)，而 $\sigma_1,\sigma_2,\cdots,\sigma_m$ 是P中的任意元，则存在一个 $A\in\mathfrak{A}$ 使 $\rho_i A=\sigma_i$，$(i=1,2,\cdots,m)$. 应用此结果另证定理2.

2. 设P是域 Φ 的任一扩张域，证明：若 $\alpha\in\mathrm{P}$ 对于一切 $A\in\mathfrak{L}_\Phi(\mathrm{P},\mathrm{P})$ 满足条件 $\alpha_R A=A\alpha_R$，则 $\alpha\in\Phi$.

3. 设 $(\rho_1,\rho_2,\cdots,\rho_n)$ 是 P/Φ 的一个基，$(A_1,A_2,\cdots,A_n)$ 是P上 $\mathfrak{L}_\Phi(\mathrm{P},\mathrm{P})$ 的一个右基，证明：$n\times n$ 矩阵 $(\rho_i A_j)$ 在 P_n 中有一个逆元素.

3. 域的同构的戴得金（Dedekind）无关定理 设 s 是域 E 到域 P 内的一个同构，则 s 是 E 的加群 $(E, +)$ 到 $(P, +)$ 内的一个同构且满足乘法条件 $(\varepsilon\eta)^s = \varepsilon^s\eta^s$. 我们可将它写成算子形式：

(2) $$\eta_R s = s(\eta^s)_R,$$

这里 η_R 是 E 中用 η 乘的乘法，而 $(\eta^s)_R$ 是 P 中用 η^s 乘的乘法. 若 E 及 P 二者都是 Φ 上的域，则 E/Φ 到 P/Φ 内的一个同构是第一个代数到第二个代数内的一个代数同构. 因此，除了条件

$$(\varepsilon+\eta)^s = \varepsilon^s + \eta^s,\ (\varepsilon\eta)^s = \varepsilon^s\eta^s,\ 1^s = 1,$$

s 是 1—1 的元外，我们还有 $(\alpha\varepsilon)^s = \alpha\varepsilon^s$ 对于 $\alpha\in\Phi$ 成立. 这些条件的第一个与最后一个恰是 $s\in\mathfrak{L}_\Phi(E, P)$ 的条件. 因此如果 s 是 E/Φ 到 P/Φ 内的同构，则 $\alpha^s = (\alpha 1)^s = \alpha 1^s = \alpha$ 对每个 $\alpha\in\Phi$ 成立. 反之，由这个条件推出 $(\alpha\varepsilon)^s = \alpha\varepsilon^s$, $\varepsilon\in E$. 所以 E/Φ 到 P/Φ 内的同构恰是 E 到 P 内的同构，它对于 Φ 来说则是 Φ 上的恒等映射.

现在我们将推导联系 E 到 P（不带有 Φ 的！）内的同构的线性关系的两个基本结果：

定理 3（戴得金）. 设 E 及 P 是域，而 $s_1, s_2, \cdots, s_n$ 是 E 到 P 内的不同的同构，则如果 s_i 是 P 上右线性无关的：$\Sigma s_i\rho_i = 0$, $\rho_i\in P$, 那么每个 $\rho_i = 0$, 这里 $s\rho \equiv s\rho_R$.

证 如果结论不成立，那么我们有一个最短关系，适当改变编号后可写成：

(3) $$s_1\rho_1 + s_2\rho_2 + \cdots + s_r\rho_r = 0,$$

这里每个 $\rho_i \neq 0$. 假设 $r > 1$, 由于 $s_1 \neq s_2$, 存在 $\eta\in E$ 使 $\eta^{s_1}\neq\eta^{s_2}$. 现以 η_R 左乘(3)，由(2)可得 $s_1\eta^{s_1}\rho_1 + s_2\eta^{s_2}\rho_2 + \cdots + s_r\eta^{s_r}\rho_r = 0$. 然后用 η^{s_1} 右乘(3)可得 $s_1\rho_1\eta^{s_1} + s_2\rho_2\eta^{s_1} + \cdots + s_r\rho_r\eta^{s_1} = 0$. 将这两个新关系相减得

$$s_2\rho_2(\eta^{s_2} - \eta^{s_1}) + s_3\eta_3(\eta^{s_3} - \eta^{s_1}) + \cdots = 0.$$

因为 $\rho_2(\eta^{s_2} - \eta^{s_1}) \neq 0$, 这是一个较(3)更短的非平凡关系. 因此只能有 $r = 1$, 即 $s_1\rho_1 = 0$. 由于 ρ_{1R}^{-1} 存在，故 $s_1 = 0$, 这与

s_i 是一个同构的假设矛盾.

将定理 1 与戴得金定理结合起来可得如下结论

推论. 设 E 及 P 是 Φ 上的域且 $[E:\Phi]=n<\infty$, 则最多存在 n 个 E/Φ 到 P/Φ 内的不同的同构.

证 令 $s_1, s_2, \cdots, s_r$ 是 E/Φ 到 P/Φ 内的不同的同构, 则它们是 $\mathfrak{L}_\Phi(E, P)$ 的右 P 无关元; 由于 $[\mathfrak{L}_\Phi(E, P):P]_R=n$, 我们只能有 $r \leqslant n$.

下节将考虑一个由域的有限多个自同构生成的右 P 向量空间. 更一般地, 设 $s_1, s_2, \cdots, s_n$ 是 E 到 P 内的不同的同构, 而 $\mathfrak{A}$ 是如下形式的自同态的集:

$$s_1\rho_1+s_2\rho_2+\cdots+s_n\rho_n, \quad \rho_i \in P. \tag{4}$$

显然 $\mathfrak{A}$ 是右 P 向量空间 $\mathfrak{L}(E, P)$ 的一个子空间. 而且, 若 $\varepsilon \in E$, 则由(2)有 $\varepsilon_R s_i=s_i(\varepsilon^{s_i})_R$, 因此

$$\varepsilon_R\left(\sum_1^n s_i\rho_i\right)=\sum_1^n s_i(\varepsilon^{s_i})_R\rho_i=\sum_1^n s_i(\varepsilon^{s_i}\rho_i).$$

这表示 $\mathfrak{A}$ 在用任意 $\varepsilon_R(\varepsilon \in E)$ 左乘下是封闭的,我们需要以下的结论

定理 4. 设 E 及 P 是两个域, $s_1, s_2, \cdots, s_n$ 是 E 到 P 内的同构, $\mathfrak{A}$ 是自同态 $\Sigma s_i\rho_i(\rho_i \in P)$ 组成的 $\mathfrak{L}(E, P)$ 的右 P 子空间, $\mathfrak{B}$ 是 $\mathfrak{A}$ 的一个 P 子空间,它在用元 $\varepsilon_R(\varepsilon \in E)$ 左乘下不变,则

$$\mathfrak{B}=s_{i_1}P+s_{i_2}P+\cdots+s_{i_r}P\left(=\left\{\sum_j s_{i_j}\rho_{i_j}\right\}\right),$$

这里 $\{s_{i_1}, s_{i_2}, \cdots, s_{i_r}\}=\mathfrak{B}\cap\{s_1, s_2, \cdots, s_n\}$.

证 显然 $\left\{\sum_{j=1}^r s_{i_j}\rho_{i_j} \mid \rho_{i_j} \in P\right\} \subseteq \mathfrak{B}$. 要证反包含只要证明: 若 $\sum_1^n s_i\rho_i \in \mathfrak{B}$, 则 $\rho_i \neq 0$ 的 s_i 必包含于 $\mathfrak{B}$ 中即可. 如若不然, 则在 $\mathfrak{B}$ 中有一元 $s_{k_1}\rho_{k_1}+s_{k_2}\rho_{k_2}+\cdots+s_{k_s}\rho_{k_s}$, 其中每个 $\rho_{k_t} \neq 0$, 而 $s_{k_t} \notin \mathfrak{B}$, 我们就能象戴得金定理的证法一样,假设 s 为极小,若 $s>1$, 我们应用前面已经用过的步骤去求得一个包含于 $\mathfrak{B}$ 内的

同一类型的更短元。因此 $s_{k_1}\rho_{k_1} \in \mathfrak{B}$，而这又推得 $s_{k_1} \in \mathfrak{B}$，与原假设矛盾。

习　题　5

1.设 $E=\Phi(\theta)$，这里的 θ 是 Φ 上的代数元，$(f(x))$ 是同态 $g(x)\to g(\theta)$ 的核（卷 1 的中译本 p.96），则 $[E:\Phi]=\deg f$. 利用导言中的扩张定理V证明 E/Φ 到 P/Φ 内的同构的个数不超过 $\deg f$. 推广此结果以得到定理 3 推论的另一证法.

4. 有限自同构群　设 G 是域 P 的一个自同构群，Φ 是 P 的元 α 的子集，这里 $\alpha^s=\alpha$ 对于每个 $s\in G$ 均能成立. 我们将称 Φ 为 P 的 G 不变元集. 由于一个自同构的不变元(或固定元)组成一子域，所以 Φ 是 P 的一个子域，我们把它记作 $\Phi=I(G)$（若要指出 P 则可表为 $I_P(G)$），并称这种形式的子域(即一自同构群的不变元的子域）为 P 中的伽罗瓦子域，而称 P 在 Φ 上为伽罗瓦域或 P/Φ 为伽罗瓦域.

我们刚才指出的过程把自同构群 G 与子域 $I(G)$ 联系了起来，并且有这些群到 P 的子域的映射 $G\to I(G)$. 现在来定义一个相反方向的映射：若 Φ 是 P 的任一子域，则我们使 Φ 与由 P/Φ 的自同构构成的集 $A(\Phi)$（或 $A_P(\Phi)$、即 P 的能使 $\alpha^s=\alpha$ 对于所有 $\alpha\in\Phi$ 都能成立的自同构 s 的集）对应. 显然，$A(\Phi)$ 是 P 的全部自同构的群 A 的一个子群，我们称 $A(\Phi)$ 是 P/Φ 的伽罗瓦群. 我们有子域到群的映射 $\Phi\to A(\Phi)$，映射 $G\to I(G)$，$\Phi\to A(\Phi)$ 的下列性质容易由定义推得：

(α) $G_1\supseteq G_2 \Rightarrow I(G_1)\subseteq (G_2)$（$\Rightarrow$ 表示"推出"）.

(β) $\Phi_1\supseteq\Phi_2 \Rightarrow A(\Phi_1)\subseteq A(\Phi_2)$.

(γ) $I(A(\Phi))\supseteq\Phi$.

(δ) $A(I(G))\supseteq G$.

这些关系有以下结果：

(ε) $I(A(I(\Phi)))=I(G)$.

(η) $A(I(A(\Phi)))=A(\Phi)$.

这两式的证明是相同的，所以仅考虑 (ε)：对 $\Phi=I(G)$ 应用

(γ) 可得 $I(A(I(G))) \supseteq I(G)$；另一方面，若应用 (α)[1] 到 $A(I(G))\supseteq G$ 上去，我们又可得到 $I(G)\supseteq I(A(I(G)))$. 故 (ε) 成立. (ε) 的一个推论是：Φ 是 P 中的伽罗瓦子域当且仅当 Φ 是 P/Φ 的伽罗瓦群的不变元的集，即 $\Phi = I(A(\Phi))$. 显然这个条件是充分的；另一方面，若 $\Phi = I(G)$ 是对应于某个自同构群 G 的子域，则 $\Phi = I(G) = I(A(I(G))) = I(A(\Phi))$.

我们现在从有限自同构群出发来研究伽罗瓦对应 $\Phi \to A(\Phi)$，$G \to I(G)$. 我们用 $(G:1)$ 表示一个群 G 的阶，更一般地用 $(G:H)$ 表示 G 中一个子群 H 的指数. 我们将从贾柯勃逊-布尔巴基定理（定理 2）出发得到子域-群对应的全部结果. 先证如下

引理. 设 G 是域 P 中的一个有限自同构群，令

$$\mathfrak{A} = \left\{\sum_{1}^{n} s_i\rho_i \,\middle|\, s_i \in G,\ \rho_i \in P\right\}$$，则 $\mathfrak{A}$ 满足定理 2 的假设 (i)，(ii)，(iii)，$[\mathfrak{A}:P]_R = (G:1)$，且定理 2 给出的子域 Φ 是 G 不变元子域，若 $\mathfrak{B}$ 是 $\mathfrak{A}$ 的一个子环及 P 上的 $\mathfrak{A}$ 的一个子空间，则

$$\mathfrak{B} = \left\{\sum_{1}^{r} t_j\rho_j \,\middle|\, t_j \in H,\ \rho_j \in P\right\},$$

这里的 $H = \{t_j\}$ 是 G 的一个子群.

证　若 $\rho \in P$，且 s 是一个自同构，则(2)表明 $\rho_R s = s(\rho^s)_R$，因此 $(s_i\rho_i)(s_j\rho_j) = s_i(\rho_{iR}s_j)\rho_{jR} = s_is_j(\rho_i^{s_j})_R\rho_{jR} = s_is_j\rho_i^{s_j}\rho_j \in \mathfrak{A}$，这是因为 $s_is_j \in G$. 由此推得 $\mathfrak{A}$ 是自同态环 $\mathfrak{L}(P, P)$ 的一个子环，由于 $1 \in G$ 及 $G\subseteq\mathfrak{A}$，故 $1 \in \mathfrak{A}$. 易见 $\mathfrak{A}$ 是 P 上右向量空间 $\mathfrak{L}(P,P)$ 的一个子空间. 由戴得金定理，可知 s_i 是在 P 上无关的.

$$[\mathfrak{A}:P]_R = (G:1) < \infty.$$

定理 2 的子域 Φ 是使 $\alpha_R A = A\alpha_R$ 对所有 $A \in \mathfrak{A}$ 成立的 $\alpha \in P$ 的集. 由于 $\alpha_R\rho_R = \rho_R\alpha_R$，$\rho \in P$ 总成立，所以这个条件等价于 $\alpha_R s_i = s_i\alpha_R$，$s_i \in G$. 因为 $\alpha_R s_i = s_i(\alpha^{s_i})_R$，这又等价于 $s_i(\alpha^{s_i})_R = s_i\alpha_R$，$s_i \in G$. 因为 s_i^{-1} 存在，这又变成 $(\alpha^{s_i})_R = \alpha_R$ 或 $\alpha^{s_i} = \alpha$，

---

1) 原书此处误为 I——译者注.

它表示 $\alpha_R A = A\alpha_R$，$A \in \mathfrak{A}$，等价于：α 是 G 不变元．现设 $\mathfrak{B}$ 是 $\mathfrak{A}$ 的一个子环，同时也是一个 P 子空间，则 $\mathfrak{B} \supseteq 1\mathrm{P} = \{\rho_R | \rho \in \mathrm{P}\}$，从而 $\mathfrak{B}$ 在用 ρ_R 左乘下是不变的．故由定理 4，

$$\mathfrak{B} = t_1\mathrm{P} + t_2\mathrm{P} + \cdots + t_r\mathrm{P}，\text{其中，} H = \{t_j\} = G \cap \mathfrak{B}.$$

显然 $H = G \cap \mathfrak{B}$ 关于乘法是封闭的，因此是 G 的一个有限子半群，从而 H 是 G 的一个子群．

关于一个域的有限自同构群的主要结果是

定理 5. 设 P 是一个域，$\mathscr{A}$ 是 P 中有限自同构群的类，$\mathscr{I}$ 是 P 的子域的类，这些子域是伽罗瓦的且在 P 中是有限余维数的．若 $\Phi \in \mathscr{I}$，则令 $A(\Phi)$ 为 P/Φ 的伽罗瓦群；若 $G \in \mathscr{A}$，则取 $I(G)$ 为 P 的 G 不变元素子域，则：(i) 若 $\Phi \in \mathscr{A}$，则 $A(\Phi) \in \mathscr{A}$；而若 $G \in \mathscr{A}$，则 $I(G) \in \mathscr{I}$．此外，还有 $I(A(\Phi)) = \Phi$，$A(I(G)) = G$．(ii) 若 $G \in \mathscr{A}$，则 $(G:1) = [\mathrm{P}:I(G)]$．(iii) 若 $\Phi \in \mathscr{I}$ 且 E 是 P 的包含 Φ 的一个子域，则 $E \in \mathscr{I}$．(iv) 在这种情况下 $H = A(E)$ 是 $G = A(\Phi)$ 的一个子群，它在 G 中不变当且仅当 E 是 Φ 上的伽罗瓦域．此时 E/Φ 的伽罗瓦群 $A_E(\Phi)$ 同构于 G/H．

证 (i)—(ii)：若 $G \in \mathscr{A}$ 且 $\mathfrak{A} = \{\Sigma s_i\rho_i | s_i \in G,\ \rho_i \in \mathrm{P}\}$，则由引理及定理 2 有 $[\mathrm{P}:I(G)] = [\mathfrak{A}:\mathrm{P}]_R = (G:1)$．若令 $\Phi = I(G)$，而 $G' = A(\Phi)$ 是 P/Φ 的伽罗瓦群，则戴得金定理的推论表明 $(G':1) \leqslant [\mathrm{P}:\Phi] = (G:1)$．由于 $G \subseteq G'$ 是显然的，故 $G' = G$，因此 $A(I(G)) = G$．然后令 Φ 是伽罗瓦的及在 P 中为有限余维数的子域，则 $\Phi = I(G)$，这里的 G 是 P/Φ 的伽罗瓦群，由戴得金定理的推论可知它是有限的，因此 $A(\Phi) \in \mathscr{A}$ 且 $I(A(\Phi)) = \Phi$，这就完成了 (i) 与 (ii) 的证明．(iii)：设 $\Phi \in \mathscr{I}$，$\mathfrak{A}$ 是由 P/Φ 的伽罗瓦群 G 确定的自同态环，由定理 2，$\mathfrak{A} = \mathfrak{L}_\Phi(\mathrm{P}, \mathrm{P})$．现设 E 为 P 的包含 Φ 的一个子域，则 $\mathfrak{B} = \mathfrak{L}_E(\mathrm{P}, \mathrm{P})$ 是 $\mathfrak{A}$ 的一个子环，且属引理所考虑的类型．因此 $\mathfrak{B} = t_1\mathrm{P} + \cdots + t_r\mathrm{P}$，其中 $H = \{t_j\}$ 是 G 的一个子群．由于 $E = \{\varepsilon | \varepsilon_R B = B\varepsilon_R,\ B \in \mathfrak{B}\}$，可知 E 是 H 不变元子域．这就证明了 (iii)．(iv) 若

$s\in G$，E 在 s 下的象 E^s 是 P 的包含 Φ 的另一个子域，则由定义直接可得 $A(E^s)=s^{-1}Hs$。因此 H 在 G 中是不变的当且仅当 $E^s=E$ 对每个 $s\in G$ 成立。我们现在证明这当且仅当 E 是 Φ 上的伽罗瓦域时成立，而且此时有 $A_E(\Phi)\cong G/H$：首先假设 $E^s=E$，而且设 G' 是 $s\in G$ 在 E 上的限制 s' 的群，则 G' 是 E 的一个有限自同构群而且 $I(G')=\Phi$，因此 Φ 是 E 的伽罗瓦子域而且将 (i) 应用于 E 可得

$$G'=A_E(\Phi).$$

映射 $s\to s'$ 是 G 到 G' 上的一个同态，其核是在 E 上使 $s'=1$ 的 $s\in G$ 的集，此集就是 H，因此 $G'\cong G/H$。次设 E 是 Φ 上的伽罗瓦扩域，则我们有 $[E:\Phi]$ 个不同的 E 在 Φ 上的自同构，而且可将它们看做 E/Φ 到 P/Φ 内的同构。另一方面，由戴得金定理的推论可知最多只有 $[E:\Phi]$ 个 E/Φ 到 P/Φ 内的同构，因此它们必须与 E/Φ 的自同构相同。若 $s\in G$，s 在 E 上的限制是 E/Φ 到 P/Φ 内的一个同构，因此这是一个自同构。这就推得 $E^s=E$ 对于一切 $s\in G$ 成立。

特别地，定理 5 在 P 的包含一个固定子域 Φ、且在 P 中是伽罗瓦的有限余维数子域 E 的类与 P/Φ 的伽罗瓦群 G 的子群 H 的类之间建立了一个双射（即 1—1 的、到上的映射），这个对应满足 (iii) 及 (iv) 中的各性质。我们还须指出 $\{H\}$ 是有限的，这就是说 P 及 Φ 间的域的类是有限的。在这点上我们的理论存在一个严重的缺陷，因为我们还没有给出 P 是 Φ 上的有限维伽罗瓦域的条件。下面三节我们将弥补这个缺陷以便将现在讨论的"抽象的"伽罗瓦理论与方程论连接起来。

习 题 6

1. 设 C 为复数域，$\mathrm{P}=C(\xi)$ 为 C 的一个单超越扩张（卷 1 的中译本 p.94），s 是 P/C 的使 $\xi^s=\varepsilon\xi$ 的自同构（这里 ε 是一个 n 次本原单位根），t 是 P/C 的使 $\xi^t=\xi^{-1}$ 的自同构。证明 $s^n=1$，$t^2=1$，$st=ts^{-1}$，而且由 s，t 生成的自同构群 G 是 $2n$ 阶的。证明其 G 不变元子域是 $C(\eta)$，$\eta=\xi^n+\xi^{-n}$。

2. 确定 Φ 上的 $\Phi(\rho)$ 的伽罗瓦群，这里的 Φ 是有理数域而 $\rho^4=2$。

3.设 P 是 Φ 上的有限维伽罗瓦域，假设其伽罗瓦群 $G = G_1 \times G_2$，这里 G_i 是 G 的子群. 证明：若 P_i 是对应于 G_i 的子域，则 P_i/Φ 是伽罗瓦子域，而且 $P = P_1 \otimes P_2$ (Φ 上的).

4.设 Φ 是特征 $\neq 2$ 的域，P 是一个扩张域：$[P:\Phi] = 2$，证明：$P = \Phi(\theta)$，这里 $\theta^2 = \alpha \in \Phi$. 利用这个结果证明 P 是 Φ 上的伽罗瓦域.

5.证明：若 Φ_1 及 Φ_2 是 P 内的伽罗瓦子域，则 $\Phi_1 \cap \Phi_2$ 是 P 内的伽罗瓦子域. 设 Φ 是特征为 0 的域，$P = \Phi(\xi)$，ξ 是超越元，而设 $\Phi_1 = \Phi(\xi^2)$，$\Phi_2 = \Phi(\xi(\xi+1))$. 证明 $[P:\Phi_1] = 2 = [P:\Phi_2]$ 但 $[P:\Phi_1 \cap \Phi_2]$ 却是无限的.

6.证明，若 R_0 是有理数域，则 $R_0(\sqrt[3]{2})$ 不是 R_0 上的伽罗瓦域.

7.设 G 是域 P 的任一自同构群，$\mathfrak{A} = \{\Sigma s_i \rho_i | s_i \in G, \rho_i \in P\}$. 证明 $\mathfrak{A}$ 满足定理 2 的假设 (i) 及 (ii). 而且 $\Phi = \{\alpha | \alpha_R A = A\alpha_R, A \in \mathfrak{A}\}$ 是 G 不变元子域. 利用这些结果及 §2 习题的第 1 题证明：若 E 是 P 的包含 Φ 且 $[E:\Phi] < \infty$ 的一个子域，则 E/Φ 到 P/Φ 内的任一同构能扩张成 P/Φ 的一个自同构.

8.(卡普兰斯基 (Kaplansky)). P, Φ, E 及 G 如第 7 题所示，证明 E 是 P 的伽罗瓦子域(换言之，若 Φ 是 P 的伽罗瓦子域且 $E \supseteq \Phi$ 满足 $[E:\Phi] < \infty$，则 E 是 P 的伽罗瓦子域). (提示：令 $H = G \cap A(E)$，设 Δ 是 P/Φ 的包含 E 的有限维子空间，利用 §2 习题中的第 1 题证明 $\mathfrak{L}_\Phi(\Delta, P)$ 有一个形如 $(\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_n)$ 的右 P 基，这里的 $\bar{s}_i$ 是 $s_i \in G$ 在 Δ 上的限制. 利用定理 4 证明 $\mathfrak{L}_E(\Delta, P)$ 有一个 P 基 $(\bar{t}_1, \bar{t}_2, \cdots, \bar{t}_r)$，$t_i \in H$. 利用这结果及 §2 习题中的第 2 题证明 $E = I(H)$.)

5. 多项式的分裂域 设 Φ 是一个给定的域，而 $f(x)$ 是一个包含在多项式环 $\Phi[x]$ 中的非零多项式，这里 x 是一个未定元. 我们知道 Φ 的一个元 ρ 称为 $f(x)$ 或方程 $f(x) = 0$ 的根如果 $f(\rho) = 0$，这当且仅当在 $\Phi[x]$ 中有 $f(x) = (x-\rho)g(x)$ (卷 1 的中译本 p.93)；而且如果 $\deg f(x) = n$，则 $f(x)$ 在 Φ 中至多只有 n 个根 (卷 1 的中译本 p.97). 设 $\rho_1, \rho_2, \cdots, \rho_r$ 是不同的根，则

$$f(x) = (x-\rho_1)(x-\rho_2)\cdots(x-\rho_r)g(x).$$

在卷 1 的中译本 pp.94—95 中，我们已经给出了扩张 P/Φ 的构造，在其中一已知不可约多项式 $f(x) \in \Phi[x]$ 有一个根. 若将这结论应用到任一非零多项式 $f(x) \in \Phi[x]$ 的一个不可约因子上去，我们就可得到一个包含 $f(x)$ 的一个根的扩张 P/Φ. 我们现在将证明最小扩张域 P 的存在性，在其中一已知的次数大于零的多项式 $f(x)$ 能分解成线性因子的乘积. 如不另加申明，我们总假设我们的多项式的首项系数为 1，因此我们需要一个扩张 P/Φ，使在

P(x) 中有

$$(5)\qquad f(x)=(x-\rho_1)(x-\rho_2)\cdots(x-\rho_n).$$

若 $\Phi(\rho_1,\rho_2,\cdots,\rho_n)$ 表示 P/Φ 的由 ρ_i 生成的子域，则显然分解式(5)在 $\Phi(\rho_1,\rho_2,\cdots,\rho_n)[x]$ 中也成立，因此，若 P/Φ 是最小的，则必有 $P=\Phi(\rho_1,\rho_2,\cdots,\rho_n)$. 我们知道若不计 Φ 中的因子则在 $P[x]$ 中分解(5)是唯一的(卷 1 的中译本 p.94 及 p.114). 由此可推得：集 $\{\rho_i\}$ 是 $f(x)$ 在 P 中的根的完全系，又若 Σ/Φ 是 $\Phi(\rho_1,\cdots,\rho_n)/\Phi$ 的一个子域使 $f(x)$ 是 $\Sigma[x]$ 中线性因子的积，则 $\Sigma=\Phi(\rho_1,\rho_2,\cdots,\rho_n)$. 由此我们给出下列定义

定义 1. 设 Φ 是一个域而 $f(x)$ 是系数在 Φ 中的正次数首项系数为 1 的多项式，则扩张域 P/Φ 称为 $f(x)$ 的一个分裂域，如果分解式(5)在 $P(x)$ 中成立且 $P=\Phi(\rho_1,\rho_2,\cdots,\rho_n)$.

我们直接可以得到两个常用的结果：

引理 1. (1)若 P/Φ 是 $f(x)\in\Phi[x]$ 的一个分裂域，而 Σ/Φ 是 P/Φ 的一个子域，则 P/Σ 是 $f(x)$ 的一个分裂域. (2)若 P/Σ 是 $f(x)\in\Phi[x]$ 的一个分裂域而且 $\Sigma=\Phi(\sigma_1,\cdots,\sigma_r)$, 这里 $f(\sigma_i)=0$, 则 P/Φ 是 $f(x)$ 的一个分裂域.

证 (1) 这是定义的直接结果.

(2) 由假设有 $P=\Sigma(\rho_1,\rho_2,\cdots,\rho_n)$, 在 $P[x]$ 中 (5) 成立. 还因 $\Sigma=\Phi(\sigma_1,\cdots,\sigma_r)$ 及 $f(\sigma_j)=0$, 故知每个 σ_j 是 ρ_i 中的一个，因此 $P=\Phi(\rho_1,\rho_2,\cdots,\rho_n)$.

现在我们可以证明以下的存在定理：

定理 6. 任一正次数多项式 $f(x)\in\Phi[x]$ 都有一个分裂域 P/Φ.

证 设 $f(x)=f_1(x)f_2(x)\cdots f_k(x)$ 是 $f(x)$ 的(首项系数为 1 的)不可约因子分解，显然 $k\leqslant n=\deg f(x)$. 我们对 $n-k$ 应用归纳法：若 $n-k=0$, 则所有 $f_i(x)$ 的次数都为 1，这说明 Φ 本身已是一个分裂域. 现设 $n-k>0$, 因此有某个 f_i 例如 $f_1(x)$ 的次数 >1, 则存在一个扩张域 E/Φ 使 $E=\Phi(\rho)$ 且 $f_1(\rho)=0$. 于是在 $E[x]$ 中 $f_1(x)=(x-\rho)f_1^*(x)$, 从而

$f(x)$ 在 $E[x]$ 中是 $l>k$ 个不可约因子的乘积，故 $n-l<n-k$，由归纳假定，对于 $f(x)$ 存在一个分裂域 P/E. 由于 $E=\Phi(\rho)$，引理表明 P/Φ 是 $f(x)$ 的一个分裂域.

我们看分裂域的几个例子.

(1) $f(x)=x^2+\alpha x+\beta$. 若 f 在 $\Phi[x]$ 中可约，则 Φ 是一个分裂域；否则可令 $P=\Phi[x]/(f(x))$，由于 f 是不可约的，故 P 是一个域. 今令 $\rho_1=x+(f(x))$，这里的 $(f(x))$ 按惯例表示由这个多项式生成的主理想，则在 P 中 $f(\rho_1)=0$，因此在 $P[x]$ 中 $f(x)=(x-\rho_1)(x-\rho_1)$. 故 $P=\Phi[\rho_1]=\Phi(\rho_1)$ 是一个分裂域，由于 $f(x)$ 是 ρ_1 的最小多项式，由导言的 VIII 知 $[P:\Phi]=2$.

(2) 设 p 为素数，而 $f(x)=x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$，$\Phi=R_0$ 是有理数域，则 P 是 $f(x)$ 的一个分裂域当且仅当它是 $g(x)=x^{p-1}+x^{p-2}+\cdots+1$ 的一个分裂域. 我们早已知道 $g(x)$ 是不可约的（卷 1 的中译本 p.118 习题 50 的第 2 题）. 因此 $P=R_0[x]/(g(x))$ 是 R_0 上的一个域而且 $P=R_0[\rho]=R_0(\rho)$，$\rho=x+(g(x))$. 我们有 $\rho^p=1$，$\rho\neq1$. 由此可推出 ρ 在 P 的乘群 P^* 中是 p 阶的. 因此 $1,\rho,\rho^2,\cdots,\rho^{p-1}$ 是互异的且全部是 $x^p-1=0$ 的根. 由此推得

$$x^p-1=\prod_{j=0}^{p-1}(x-\rho^j),\ \text{从而}\ P=R_0(\rho)$$

是一个分裂域.

(3) $f(x)=(x^2-2)(x^2-3)$，$\Phi=R_0$，我们先作 $E=R_0(\rho)$，这里的 $\rho^2=2$. 我们知道 x^2-2 在 $R_0[x]$ 中是不可约的（欧几里得）. 在 E 中我们有 $x^2-2=(x-\rho)(x+\rho)$. 又 x^2-3 在 $E[x]$ 中是不可约的，否则存在 $\eta\in E$ 使 $\eta^2=3$. 设 $\eta=\alpha+\beta\rho$，其中 α，β 是有理数，$\eta^2=(\alpha^2+2\beta^2)+2\alpha\beta\rho$. 若它等于 3，则有 $\alpha\beta=0$ 及 $\alpha^2+2\beta^2=3$；这时若 $\beta=0$，我们将有 $\alpha^2=3$；这时若 $\alpha=0$，我们又将有 $\beta^2=\frac{3}{2}$. 这二者对于有理数都是不可能的. 作 $P=E(\eta)$，这里的 $\eta^2=3$. 这时我们有 $P=R_0(\rho,\eta)$ 而在 $P[x]$ 中，$(x^2-2)(x^2-3)=(x-\rho)(x+\rho)\times(x-\eta)(x+\eta)$，故 P/R_0 是一个分裂域，应用导言中的 VI 及 VIII，可见 $[P:\Phi]=4$.

在继续讨论分裂域以前把关于域扩张以及域 Φ 的代数扩张的某些记法固定下来是适宜的，它们在某种程度上早已被采用. 若 S 是域 P/Φ 的一个子集，则我们用 $\Phi[S]$ 及 $\Phi(S)$ 分别表示 Φ 上由 S 生成的子代数及子域. 由定义可见，前者是 P/Φ 的包含 S 的所有子代数之交，而后者则是 P/Φ 的包含 S 的所有子域之交. 显然 $\Phi[S]$ 是 Φ 上 P 的由 1 及所有单项式 $\sigma_1\sigma_2\cdots\sigma_m(\sigma_i\in S)$ 生成的子空间，而 $\Phi(S)$ 则是元 $\alpha\beta^{-1}$ 的集，这里 α，$\beta\in\Phi[S]$，

$\beta \neq 0$. 由定义直接可得：若 S_1 及 S_2 是 P 的子集，则

$$(\Phi(S_1))(S_2) = \Phi(S_1 \cup S_2),$$

此式左端当然是由 S_2 生成的 $P/\Phi(S_1)$ 的子域.

若 ρ 是 P/Φ 的一个代数元，则 $[\Phi[\rho]:\Phi] = \deg f(x)$，这里的 $f(x)$ 是 ρ 在 Φ 上的最小多项式(导言的 VIII). 事实上，我们已经知道，若 $\deg f(x) = n$，则 $(1, \rho, \rho^2, \cdots, \rho^{n-1})$ 是 P/Φ 的一组基. 由于维数 $[\Phi[\rho]:\Phi]$ 是有限的，故 $\Phi(\rho)$ 是一个域(导言的 VII). 因此显然有 $\Phi(\rho) = \Phi[\rho]$. 我们将推广这些结果，证明下列关于逐次代数扩张的关键引理.

引理 2. 设 $P = \Phi(\rho_1, \rho_2, \cdots, \rho_m)$ 而且 ρ_i 是 $\Phi(\rho_1, \rho_2, \cdots, \rho_{i-1})$ $(i = 1, 2, \cdots, m)$ 上的代数元，则 $[P:\Phi] < \infty$ 且 $P = \Phi[\rho_1, \rho_2, \cdots, \rho_m]$.

(我们将在后面(p.247)看到其逆定理：若 $P = \Phi[\rho_1, \rho_2, \cdots, \rho_n]$ 是一个域，则 ρ_i 是 Φ 上的代数元).

证 我们已看到命题在 $m = 1$ 时成立. 假设 $m > 1$ 且此结果在 $r < m$ 时成立，则 $\Phi(\rho_1, \rho_2, \cdots, \rho_r) = \Phi[\rho_1, \rho_2, \cdots, \rho_r]$ 且它在 Φ 上是有限维的. 由于 ρ_{r+1} 是 $\Phi(\rho_1, \rho_2, \cdots, \rho_r)$ 上的代数元，我们有 $\Phi(\rho_1, \cdots \rho_r)(\rho_{r+1}) = \Phi(\rho_1, \cdots, \rho_r)[\rho_{r+1}]$. 且此扩张在 $\Phi(\rho_1, \cdots, \rho_r)$ 上的维数是有限的. 由此推得

$$\begin{aligned}(6)\qquad [\Phi(\rho_1, \cdots, \rho_{r+1}):\Phi] &= [\Phi(\rho_1, \cdots, \rho_r)(\rho_{r+1}):\Phi] \\ &= [\Phi(\rho_1, \rho_2, \cdots, \rho_r)(\rho_{r+1}):\Phi(\rho_1, \cdots, \rho_r)] \\ &\quad \times [\Phi(\rho_1, \cdots, \rho_r):\Phi]\end{aligned}$$

是有限的. 而且由 $\Phi(\rho_1, \cdots, \rho_{r+1}) = \Phi(\rho_1, \cdots, \rho_r)[\rho_{r+1}]$ 及 $\Phi(\rho_1, \cdots, \rho_r) = \Phi[\rho_1, \cdots, \rho_r]$ 可推出 $\Phi(\rho_1, \cdots, \rho_{r+1})$ 的每个元都是 $\rho_i (1 \leqslant i \leqslant r + 1)$ 的一个多项式，因此 $\Phi(\rho_1, \cdots, \rho_{r+1}) = \Phi[\rho_1, \cdots, \rho_{r+1}]$. 归纳即得引理.

这个结果特别在所有 ρ_i 都是 Φ 上的代数元时有用；由于 $f(x)$ 的各根 ρ_i 都是 Φ 上的代数元，显然若 P/Φ 是 $f(x) \in \Phi[x]$ 的一个分裂域，则 $[P:\Phi] < \infty$.

我们将证明一个多项式的任意两个分裂域都是 Φ 上同构的，

为了便于进行归纳论证及其他理由，最好推广这个结果如下：设 Φ 及 $\bar{\Phi}$ 是两个同构的域且 $\alpha\to\bar{\alpha}$ 是一个 Φ 到 $\bar{\Phi}$ 上的同构，我们知道这个同构可扩张成 $\Phi[x]$ 到 $\bar{\Phi}[x]$ 上的唯一同构 $f(x)\to\bar{f}(x)$，使 $x\to x$（导言的 II）。我们希望考虑多项式 $f(x)$ 在 Φ 上的一个分裂域及 $\bar{\Phi}[x]$ 中的对应多项式 $\bar{f}(x)$ 在 $\bar{\Phi}$ 上的一个分裂域，下列定理将推出分裂域的唯一性并给出一个关于分裂域的同构个数的重要结果。

定理 7. 设 $\alpha\to\bar{\alpha}$ 是域 Φ 到域 $\bar{\Phi}$ 上的一个同构，$f(x)$ 是 $\Phi[x]$ 中的正次数的首项系数为 1 的多项式，$\bar{f}(x)$ 是 $\bar{\Phi}[x]$ 中的对应多项式，P 及 $\bar{\mathrm{P}}$ 分别是 $f(x)$ 及 $\bar{f}(x)$ 在 Φ 及 $\bar{\Phi}$ 上的分裂域，则存在 P 到 $\bar{\mathrm{P}}$ 上的一个同构，它在 Φ 上与给定的同构一致。而且，若 $\bar{f}(x)$ 是 $\bar{\mathrm{P}}[x]$ 中的不同的线性因子的乘积，则由 Φ 上的给定同构扩张成 P 到 $\bar{\mathrm{P}}$ 内的同构的个数是 $[\mathrm{P}:\Phi]$。

证　这两个论断都可通过对 $[\mathrm{P}:\Phi]$ 利用归纳来证明。若 $[\mathrm{P}:\Phi]=1$，则 $\mathrm{P}=\Phi$ 而且在 $\Phi[x]$ 中 $f(x)=\Pi(x-\rho_i)$。应用 $\Phi[x]$ 的同构 $h(x)\to\bar{h}(x)$，可得 $\bar{f}(x)=\Pi(x-\bar{\rho}_i)$ 及 $\bar{\rho}_i\in\bar{\Phi}$。由此推得这些就是 $\bar{f}(x)=0$ 在 $\bar{\mathrm{P}}$ 中的根，因此 $\bar{\mathrm{P}}=\bar{\Phi}$，从而定理中的两个结果都在此情况下成立。现设 $[\mathrm{P}:\Phi]>1$，则 $f(x)$ 不是 $\Phi[x]$ 中的线性因子的乘积，因此有次数 $r>1$ 的一个不可约因子 $g(x)$，而 $\bar{g}(x)$ 是 $\bar{f}(x)$ 的一个因子。我们可设

$$g(x)=\prod_1^r(x-\rho_i),\quad \bar{g}(x)=\prod_1^r(x-\bar{\sigma}_i),$$

这里
$$f(x)=\prod_1^n(x-\rho_i),\quad \bar{f}(x)=\prod_1^n(x-\bar{\sigma}_i).$$

因为 $g(x)$ 是不可约的，它是 ρ_1 在 Φ 上的最小多项式，而且 $E=\Phi(\rho_1)$ 在 Φ 上是 r 维的（$r=\deg g>1$）。导言的扩张定理 V 推出这个同构 $\alpha\to\bar{\alpha}$ 能扩张成唯一的一个 $E=\Phi[\rho_1]=\Phi(\rho_1)$ 到 $\bar{\mathrm{P}}$ 内的同构使 $\rho_1\to\bar{\sigma}_i\ (i=1,\cdots,r)$。我们然后注意这些指定的由 E 到 P 内的同构是 $\alpha\to\bar{\alpha}$ 的仅有扩张。再由扩张定理 V，在 E 的任何同构中，若它扩张了给定的同构，则 ρ_1 被映成一个元 $\bar{\sigma}$ 使

$\bar{g}(\bar{\sigma})=0$，由于 $\bar{g}(x)=\prod_{1}^{r}(x-\bar{\sigma}_i)$，由此推得对于某个$i(1\leqslant i\leqslant r)$ 有 $\bar{\sigma}=\bar{\sigma}_i$. 因此这个同构与我们所指出的一个同构重合. 所以 $\alpha\to\bar{\alpha}$ 能扩张成 $E=\Phi(\rho_1)$ 到 $\bar{\mathrm{P}}$ 内的一个同构，而这种扩张的个数等于 $\{\bar{\sigma}_1,\cdots,\bar{\sigma}_r\}$ 中不同元的个数. 特别地，若$\bar{f}(x)$是不同的线性因子的乘积，则 $\bar{g}(x)$ 也是不同的线性因子的乘积，从而个数是 $r=\deg\bar{g}(x)=[E:\Phi]$. 我们现在用$E$代替基域$\Phi$而且选定一个扩张将$\Phi$上的同构变成$E$到$\bar{\mathrm{P}}$内的一个同构，设 $\bar{E}$ 为 E在这个扩张下的象. 用 $\varepsilon\to\bar{\varepsilon}$ 表示这个扩张，则 P/E 是$f(x)$的一个分裂域而 $\bar{\mathrm{P}}/\bar{E}$ 是 $\bar{f}(x)$的一个分裂域. 此外，$[\mathrm{P}:E]<[\mathrm{P}:\Phi]$，因为 $[E:\Phi]=r>1$，这时归纳假定表明 $\varepsilon\to\bar{\varepsilon}$ 能扩张成为P到$\bar{\mathrm{P}}$上的一个同构，且在 $\bar{f}(x)$ 是 $\bar{\mathrm{P}}(x)$ 中的不同的线性因子的一个乘积时，这种扩张的个数等于 $[\mathrm{P}:E]$. 如果我们将 $\alpha\to\bar{\alpha}$ 变到 $\varepsilon\to\bar{\varepsilon}$ 的扩张的第一个结果合起来考虑，我们就可看到存在一个扩张将同构 $\alpha\to\bar{\alpha}$ 变为P到$\bar{\mathrm{P}}$上的一个同构，而且如果 $\bar{f}(x)$ 分裂成为不同的线性因子，则我们可以得到 $[\mathrm{P}:E]\times[E:\Phi]=[\mathrm{P}:\Phi]$ 个不同的同构，这是因为我们有 $[E:\Phi]$ 个扩张到E上，而它们中的每一个又有 $[\mathrm{P}:E]$ 个扩张到P上，故我们得到 $[\mathrm{P}:\Phi]=[\mathrm{P}:E][E:\Phi]$ 个不同的扩张. 显然我们已经计入了每个扩张(参考定理 3 的推论). 证毕.

现在将这个结果运用到 $\bar{\Phi}=\Phi$ 及Φ中的恒等映射 $\alpha\to\alpha$ 这种特殊情况上去，则得结论如下：若 P/Φ 及 $\bar{\mathrm{P}}/\Phi$ 是同一多项式 $f(x)$ 的两个分裂域，则 P/Φ 及 $\bar{\mathrm{P}}/\Phi$ 必同构. 此时，结果的第二部分是：若 $f(x)$ 有不同的根，则 P/Φ 的自同构个数等于 $[\mathrm{P}:\Phi]$. 换言之，对于P/Φ 的伽罗瓦群G来说 $(G:1)=[\mathrm{P}:\Phi]$.

习　题　7

1. 构造 x^3-2 在有理数域上的一个分裂域，并求其维数.

2. 设 P/Φ 是 $\Phi[x]$ 中的 $f(x)\neq0$ 的一个分裂域而E是 P/Φ 的一个子域，证明 E/Φ 到 P/Φ 内的任一同构都能扩张成P的一个自同构.

3. 证明n次多项式 $f(x)$ 的分裂域 P/Φ 的维数不超过 $n!$.

6. 重根．可分多项式 设 $f(x)$ 是 $\Phi[x]$ 中的一个正次数多项式，P/Φ 是它的一个分裂域，将它写成

$$f(x) = (x-\rho_1)^{k_1}(x-\rho_2)^{k_2}\cdots(x-\rho_r)^{k_r}, \tag{7}$$

$\rho_i \in$ P，在 $i \neq j$ 时，$\rho_i \neq \rho_j$，我们说 ρ_i 是 $f(x)=0$ 的一个重数为 k_i 的根，简称 k_i 重根；若 $k_i = 1$，则称 ρ_i 为单根；否则称为重根．若有 Φ 上的第二个分裂域 $\bar{\text{P}}$，则在 $\bar{\text{P}}$ 中

$$f(x) = \prod_1^r (x-\bar{\rho}_i)^{k_i},$$

这里 $\rho_i \to \bar{\rho}_i$ 是 P/Φ 到 $\bar{\text{P}}/\Phi$ 上的一个同构．显然 f 的重根的存在性是与分裂域的选择无关的，下面我们将介绍一个在 $\Phi[x]$ 本身内检验重根的经典判别法，为此，我们需要 $\Phi[x]$ 中的形式导数（或微商）的概念，我们用 $(x^i)' = ix^{i-1}(i=0,1,2,\cdots; x^0 = 1)$ 在 $\Phi[x]$ 中定义一个线性映射 $f \to f'$，由于 $(1, x, x^2, \cdots)$ 是 $\Phi[x]$ 在 Φ 上的一个基，因此它定义了 $\Phi[x]$ 在 Φ 上的唯一的线性映射 $f \to f'$，我们称 f' 为 f 的（形式）导数．我们有基本法则：

$$(fg)' = f'g + fg'. \tag{8}$$

由于导数的线性性，只要在 $\Phi[x]$ 的基 (x^i) 中对 $f = x^i$，$g = x^j$ 验证就够了：$fg = x^{i+j}$，因此 $(fg)' = (i+j)x^{i+j-1}$，$f'g = ix^{i+j-1}$，$fg' = jx^{i+j-1}$，故(8)式成立，对此我们可以证明：

定理 8. 若 $f(x) \in \Phi[x]$ 且 $\deg f > 0$，则 f 的所有根（在它的分裂域内）都是单根当且仅当 $(f, f') = 1$（即 1 是 f 及 f' 的最高公因子）．

证．设 $d(x)$ 是 f 与 f' 在 $\Phi[x]$ 中的最高公因子 (f, f')（参看卷 1 的中译本 p.93，p.113），假设 $f(x)$ 在 P$[x]$ 中有一个重根，故 $f(x) = (x-\rho)^k g(x)$，$k > 1$，在 P$[x]$ 中取导数可得 $f' = (x-\rho)^k g' + k(x-\rho)^{k-1}g$，由于 $k-1 \geqslant 1$，它能被 $x-\rho$ 整除，因此 $(x-\rho) | f$（即 $x-\rho$ 是 f 的一个因子），并且 $(x-\rho)|f'$，故 $(x-\rho)|d$，因此 $d(x) \neq 1$．其次假设 f 的所有根都是单根，则有 $f(x) = \prod_1^n (x-\rho_i)$，在 $i \neq j$ 时 $\rho_i \neq \rho_j$．

通常将(8)式推广到多个因子的情形，得

$$f'(x)=\sum_{i=1}^{n}(x-\rho_1)\cdots(x-\rho_{i-1})(x-\rho_{i+1})\cdots(x-\rho_n).$$

显然由此推得 $(x-\rho_i)\nmid f'(x)$，这就得到 $(f,f')=1$.

若 f 在 $\Phi[x]$ 中是不可约的，则由 $(f,f')\neq 1$ 可推出 $f|f'$，通过考虑多项式的次数可知这仅当 $f'=0$ 时发生．若特征为 0，这显然可推出 f 是 Φ 的一个元． 若特征是 $p\neq 0$ 而且 $f(x)=\alpha_0x^n+\alpha_1x^{n-1}+\alpha_2x^{n-2}+\cdots+\alpha_n$，则 $f'(x)=n\alpha_0x^{n-1}+(n-1)\alpha_1x^{n-2}+(n-2)\alpha_2x^{n-3}+\cdots$，故由 $f'(x)=0$ 可推得 $(n-i)\alpha_i=0$，此时若整数 $n-i$ 不能被 p 整除则 $\alpha_i=0$． 由此可见 $f(x)=\beta_0x^{mp}+\beta_1x^{(m-1)p}+\cdots+\beta_m=g(x^p)$，这里 $g(x)=\beta_0x^m+\beta_1x^{m-1}+\cdots+\beta_m$． 这条件显然也是充分的，因为 $(x^{kp})'=kpx^{kp-1}=0$，所以 $f'=0$． 在特征 $p\neq 0$ 的情况下，我们将看到 f 是正次数的不可约多项式及 $f'=0$ 这二个条件有可能同时满足． 这是特征为 0 的域与特征 $p\neq 0$ 的域之间的基本区别，它就是后一情况比较复杂的根本原因．

现在更进一步考察特征 $p\neq 0$ 的域：我们还记得，若 Φ 是这种类型的域，则在 Φ 中有

(9) $$(\alpha+\beta)^p=\alpha^p+\beta^p,\ (\alpha\beta)^p=\alpha^p\beta^p,$$

(卷 1 的中译本 p.112 习题 47 的第 3 题)．第二式是显然的，第一式则是二项式定理及二项式系数 $\binom{p}{i}=p!/i!(p-i)!$ 在 $1\leqslant i\leqslant p-1$ 时能被 p 整除这一事实的结果，因为这一系数是一个整数而且 p 在分数的分子中出现但却不在分母中出现．我们还知道，若 $\alpha^p=\beta^p$，则 $(\alpha-\beta)^p=\alpha^p-\beta^p=0$，因此 $\alpha=\beta$．由此及(9)式可见映射 $\alpha\rightarrow\alpha^p$ 是 Φ 到它自身内的一个同构，它的象 $\Phi^p=\{\alpha^p|\alpha\in\Phi\}$ 组成一子域，称为***p* 次幂子域**．如果重复作这个映射 $\alpha\rightarrow\alpha^p$ 就能得到 Φ 到 p^e 次幂子域 Φ^{p^e} 上的同构 $\alpha\rightarrow\alpha^{p^e}$ $(e=1,2,\cdots)$.

我们证明下列一般结果，它在今后很有用．

引理. 若Φ是一个特征 $p\neq 0$ 的域,则 $x^p-\alpha$ 除 $\alpha=\beta^p$, $\beta\in\Phi$ 外在 $\Phi[x]$ 中是不可约的, 而在 $\alpha=\beta^p$ 时, $x^p-\alpha=(x-\beta)^p$.

证 设P是 $x^p-\alpha$ 的一个分裂域, 若β是 $x^p-\alpha=0$ 的一个根, 则 $\alpha=\beta^p$, 从而在 $P[x]$ 中, $x^p-\alpha=x^p-\beta^p=(x-\beta)^p$. 现设在 $\Phi[x]$ 中 $x^p-\alpha=g(x)h(x)$, 这里 $\deg g=k$ 且 $1\leqslant k\leqslant p-1$, 则在 $P[x]$ 中我们必有 $g=(\alpha-\beta)^k=x^k-k\beta x^{k-1}+\cdots$, 由这推得 $k\beta\in\Phi$, 因此 $\beta\in\Phi$, 从而 $x^p-\alpha=(x-\beta)^p$ 在 $\Phi[x]$ 中成立.

现在考虑下面的例子: 取 $I_p=I/(p)$ 为模p的剩余类域, 作 $\Phi=I_p(\xi)$, ξ 为超越元, 则可断言 $\xi\notin\Phi^p$. 若 $\gamma\in\Phi$, 则可写成 $\gamma=\alpha(\xi)\cdot\beta(\xi)^{-1}$, 这里 $\alpha(\xi)$ 及 $\beta(\xi)$ 都是多项式, 则 $\gamma^p=\alpha(\xi^p)\beta(\xi^p)^{-1}$, 因为由 $\alpha(\xi)=\alpha_0+\alpha_1\xi+\cdots$ 可推得 $\alpha(\xi)^p=\alpha_0^p+\alpha_1^p\xi^p+\cdots=\alpha_0+\alpha_1\xi^p+\cdots$ (弗尔马定理), 因此由 $\gamma^p=\xi$ 可推得 $\alpha(\xi^p)=\beta(\xi^p)\xi$, 由于 $1,\xi,\cdots$是 I_p 无关的, 故知这是不可能的. 因此 $\xi\notin\Phi^p$, 从而由引理, $x^p-\xi$ 在 $\Phi[x]$ 中是不可约的. 另一方面,我们已经看到 $x^p-\xi$ 在它的分裂域中有p个相等的根,此外还有 $(x^p-\xi)'=0$

今后我们把一个正次数多项式f称为**可分多项式**, 如果它是 $\Phi[x]$ 中的不可约多项式的一个乘积、这些不可约多项式在一个分裂域中都仅有单根. 我们的讨论表明: 若Φ是0特征域, 则每个 $f(x)\in\Phi[x]$ 都是可分的;而对于特征 $p\neq 0$ 的域,则存在不可分多项式.

习 题 8

1.证明引理的下列推广: $x^{p^e}-\alpha$ 是不可约的,除非 $\alpha\in\Phi^p$.

2.设 Φ_0 是有q个元的有限域, $P=\Phi_0(\xi)$, 这里ξ是 Φ_0 上的超越元,设G是P在 Φ_0 上使 $\xi\to\xi+\alpha$ $(\alpha\in\Phi_0)$ 的自同构的有限群. 证明 $\Phi=I(G)=\Phi_0(\xi^q-\xi)$.

3.设Φ是一个特征 $p\neq 0$ 的域, $\xi_1,\xi_2,\cdots,\xi_n$ 是Φ上的未定元, $P=\Phi(\xi_1,\xi_2,\cdots,\xi_n)$ 是 $\Phi[\xi_1,\xi_2,\cdots,\xi_n]$ 的分式域,证明 $[P:\Phi(\xi_1^p,\xi_2^p,\cdots,\xi_n^p)]=p^n$. 再

证明P在 $\Phi(\xi_1^{p^{e_1}}, \xi_2^{p^{e_2}}, \cdots, \xi_n^{p^{e_n}})$ 上的伽罗瓦群是单位元群.

4. 设 $P = \Phi(\xi_1, \xi_2, \cdots, \xi_n)$ 为特征 $p \neq 0$ 的域，且设 $\xi_i^{p^{e_i}} \in \Phi$ $(i = 1, 2, \cdots, n$; e_i 是一个正整数). 证明: P在 Φ 上的伽罗瓦群是单位元群.

5. 设 Φ 是一个特征 $p \neq 0$ 的域，系数在 Φ 中的一个多项式称为 p 多项式，如果它形如: $x^{p^m} + \alpha_1 x^{p^{m-1}} + \alpha_2 x^{p^{m-2}} + \cdots + \alpha_m x$. 证明: 一个首项系数为1的多项式是 p 多项式当且仅当它的各根作成其分裂域P的加群的一个子群而且所有的根有相同的重数 p^e. 再证明: 上述展开的 p 多项式的根全是单的当且仅当 $\alpha_m \neq 0$.

6. 设 $f(x)$ 在 $\Phi[x]$ 中不可约，Φ 是特征 $p \neq 0$ 的域，证明 $f(x)$ 能写成形式 $g(x^{p^e})$，这里 $g(x)$ 是不可约的而且有不同的根. 利用这个结果证明 $f(x)$ 的每个根(在一个分裂域中)有相同的重数 p^e.

7. 设 Φ 是一个0特征的域，$f(x)$ 是 $\Phi[x]$ 中的一个正次数多项式，证明: 如果 $d(x)$ 是 $f(x)$ 及 $f'(x)$ 的最高公因子，则 $g(x) = f(x)d^{-1}(x)$ 有单根，它们都是 $f(x)$ 的不同的根.

7. 伽罗瓦理论的基本定理 我们现在再回到§4的抽象伽罗瓦理论的讨论并首先回答我们在§4末提出的刻划有限维伽罗瓦扩张特性的问题，结果如下

定理 9. 一域 P/Φ 是 Φ 上的有限维伽罗瓦扩张当且仅当P是一可分多项式 $f(x) \in \Phi[x]$ 在 Φ 上的一个分裂域.

证. 设 $f(x)$ 为可分多项式，$f(x) = f_1(x)^{e_1} \cdots f_l(x)^{e_l}$，这里 $f_i(x)$ 在 $\Phi[x]$ 中不可约且当 $i \neq j$ 时 $f_i \neq f_j$，则 $f(x)_i$ 只有单根. 另外，由于 f_i 及 f_j 在 $i \neq j$ 时是不同的不可约多项式，它们的最高公因子等于1，因此 $1 = a(x)f_i(x) + b(x)f_j(x)$，$(a(x), b(x) \in \Phi[x])$. 由此推出 f_i 及 f_j 在任何扩域中均无公根，从而 $g(x) = f_1(x)f_2(x)\cdots f_l(x)$ 无重根，而且显然有: 如果 P/Φ 是 f 的一个分裂域，则它也是 g 的一个分裂域. 我们知道，任何分裂域都是有限维的，而且由定理6可以推出: 若 G 是 P/Φ 的伽罗瓦群，则 $(G:1) = [P:\Phi]$. 设 $\Phi' = I(G)$ 是 G 不变元的集，则由定理5的 (ii) 可知，$(G:1) = [P:\Phi']$. 由于 $\Phi' \supseteq \Phi$，我们有 $\Phi = \Phi'$，这就证明了 Φ 在P中是伽罗瓦的或P在 Φ 上是伽罗瓦的. 这就证明了条件的充分性. 其次假设P是 Φ 上的有限维伽罗瓦扩张而 G 是其伽罗瓦群，我们知道 G 是有限的，可记作

$$G = \{s_1, s_2, \cdots, s_n\}.$$

若 $\rho \in P$，则称它在 $s_i \in G$ 下的象 ρ^{s_i} 为 ρ 在 P/Φ 内的共轭元.

我们可设 $\rho^{s_1}, \cdots, \rho^{s_r}$ 是互异的且此集包括了全部此种共轭元，则我们可断言 $h(x) = \prod_{j=1}^{r} (x - \rho^{s_i}) \in \Phi[x]$. 要证明这一点可令 $s \in G$ 且设 s 为它在 $\mathrm{P}[x]$ 上的使 $x^s = x$ 的扩张，这样我们就有 $h^s(x) = \prod_1^r (x - \rho^{s_i s})$. 由于元 $\rho^{s_1 s}, \cdots, \rho^{s_r s}$ 是不同的共轭元，故此集是共轭元的完全系，从而 $h^s(x) = h(x)$, $(s \in G)$, 因此 $h(x) \in \Phi[x]$. 这就证明了任意元 $\rho \in \mathrm{P}$ 在 Φ 上的最小多项式(这其实是 $h(x)$) 是可分的且能分解成为 $\mathrm{P}[x]$ 中的线性因子的积. 现设 $(\rho_1, \rho_2, \cdots, \rho_n)$ 是 P/Φ 的一个基，而且 $f_i(x)$ 是 ρ_i 在 Φ 上的最小多项式，则 $f(x) = \prod f_i(x)$是可分的，而且显然 P 是 f 在 Φ 上的一个分裂域.

定理 5 讨论的伽罗瓦对应可用来论述下列结果，这个结果传统上称为

伽罗瓦理论的基本定理. 设 P 是一个可分多项式在 Φ 上的一个分裂域，G 是 P/Φ 的伽罗瓦群，对于 G 的每一个子群 H，我们令 Φ 上的 P 的 H 不变元子域 E 与之对应，而对于 Φ 上的每个子域 E 我们令 G 的子群 H 与它对应，H 由元 t 构成，而 t 对于 E 中所有的元 ε 都有 $\varepsilon^t = \varepsilon$，那末这两个对应是互逆的而且都是 G 的子群集与 P 在 Φ 上的子域集之间的双射，这两个对应关于包含关系都是反序的，而且有

$$(H:1) = [P:E], \quad (G:H) = [E:\Phi]. \tag{10}$$

此外，H 在 G 内是不变的当且仅当对应域 E 在 Φ 上是伽罗瓦的，此时 E/Φ 的伽罗瓦群同构于商群 G/H.

这里的全部结果都可由定理 5 及它后面的附注直接得出，在那里唯一没有明确指出的是公式(10)，但由定义可见 H 是 P/E 的伽罗瓦群，故 $(H:1) = [P:E]$. 又因 $(G:1) = [\mathrm{P}:\Phi]$，故

$$(G:H) = (G:1)/(H:1) = [\mathrm{P}:\Phi]/[\mathrm{P}:E] = [E:\Phi].$$

我们还要注意 $(G:H) = [E:\Phi]$ 是 E/Φ 到 P/Φ 内的不同的同构的个数，要看清这一点可考虑元 $s \in G$ 在 E 上的限制 $\bar{s}$: 对于

$s, t \in G$，若 $\bar{s} = \bar{t}$，则 $\overline{st^{-1}} = \bar{1}$，这意味着 $st^{-1} \in H$，故陪集 Hs 及 Ht 恒等．其逆可逆转以上步骤得到．由此可见集 $\{\bar{s} | s \in G\}$ 包含 $(G: H)$ 个不同的 E/Φ 到 P/Φ 内的同构．我们还知道 E/Φ 到 P/Φ 内的同构不超过 $[E:\Phi] = (G:H)$ 个（定理 3 推论），故知已取得其全部．附带地，我们还证明了 E/Φ 到 P/Φ 内的每个同构都是 P/Φ 的一个自同构的限制，换言之，任一如此的同构都能扩张成一自同构（参看 §4 习题的第 7 题）．

8. 正规扩张．正规闭包 在上节开始时我们给出了可分多项式的分裂域的一个抽象特征，它们恰是有限维伽罗瓦扩张，我们现在将给出任意分裂域的两个抽象特征．

定理10. 对于有限维扩张 P/Φ 来说，下列三条件是等价的：

(1) P/Φ 是一多项式 $f(x) \in \Phi[x]$ 的一个分裂域．

(2) P/Φ 到一扩张域 Δ/Φ 内的任何同构 s 都是一个自同构．

(3) 有一根在 P 中的每个不可约多项式 $g(x) \in \Phi[x]$ 都是 $\mathrm{P}[x]$ 中的线性因子的乘积．

证 (1)⇒(2)（“⇒”表示“可推出”）：设 $\mathrm{P} = \Phi(\rho_1, \rho_2, \cdots, \rho_n)$，在 $\mathrm{P}[x]$ 中 $f(x) = \Pi(x - \rho_i)$ 且 $f(x) \in \Phi[x]$．假设 $\Delta \supseteq \mathrm{P} \supseteq \Phi$，而 s 是 P/Φ 到 Δ/Φ 内的一个同构，由于 $f(\rho_i) = 0$，我们有 $f(\rho_i^s) = 0$，因为 $\{\rho_i\}$ 是 $f(x)$ 在 Δ 中的根的完全系，ρ_i^s 必是 ρ_i 中的某一个，因此 s 将 $\mathrm{P} = \Phi(\rho_1, \rho_2, \cdots, \rho_m)$ 的每个生成元 ρ_i 映入 P 内，故 $\mathrm{P}^s \subseteq \mathrm{P}$．由于 s 是 1—1 Φ 线性的及 $[\mathrm{P}:\Phi] < \infty$，我们有 $\mathrm{P}^s = \mathrm{P}$．故 s 是一个自同构．(2)⇒(3)：假设 P/Φ 到任何扩域 Δ/Φ 内的每个同构都是一个自同构，设 $g(x)$ 在 $\Phi[x]$ 中不可约且在 P 中有一根 σ，将 P 写成 $\mathrm{P} = \Phi(\rho_1, \rho_2, \cdots, \rho_m)$，而且 $f_i(x)$ 是 ρ_i 在 Φ 上的最小多项式，令

$$f(x) = g(x) \cdot \prod_{1}^{m} f_i(x)$$

且设 Δ/P 是 $f(x)$ 在 P 上的一个分裂域．因为 $\rho_i \in \mathrm{P}$，$f(x) \in$

$\Phi[x]$，Δ 也是 $f(x)$ 在 Φ 上的一个分裂域，而且它包含 $g(x)$ 在 Φ 上的一个分裂域，因此我们可推得：如果我们能够证明 $g(x)$ 的包含在 Δ 中的每个根 σ' 都被包含在 P 中，那么 $g(x)$ 就是 $P[x]$ 中的线性因子的乘积。在证明这命题时注意到：由于 $g(x)$ 在 $\Phi[x]$ 中是不可约的，$g(\sigma)=0=g(\sigma')$，因此存在一个 $\Phi(\sigma)/\Phi$ 到 $\Phi(\sigma')/\Phi$ 内的同构 s 使 $\sigma^s=\sigma'$。于是我们可将 Δ 看做 $f(x)=f^s(x)$ 在 $\Phi(\sigma)$ 上的及在 $\Phi(\sigma')$ 上的分裂域，因此分裂域的主要同构定理(定理6)表明 s 能扩张成为 Δ 的一个自同构 s，由于 $\alpha^s=\alpha$ $(\alpha\in\Phi)$，s 是 Δ 的一个 Φ 自同构，它在 P 上的限制是 P/Φ 到 Δ/Φ 内的一个同构，因此，由假设，这个限制是 P/Φ 的一个自同构。由于 $\sigma\in P$，故有 $\sigma^s=\sigma'\in P$，这就证明了(3)。 (3)⇒(1)：将 P 写成 $P=\Phi(\rho_1,\rho_2,\cdots,\rho_m)$，设 $f_i(x)$ 是 ρ_i 在 Φ 上的最小多项式，若(3)成立，则 $f_i(x)$ 是 $P[x]$ 中的线性因子的乘积，因此 P/Φ 是 $f(x)=\Pi f_i(x)$ 的一个分裂域。证毕。

满足定理 10 的任何一条件(因而满足全部条件)的有限维扩张 P/Φ 称为**正规扩张**。显然由条件(1)可得：若 P 是 Φ 上的正规扩张，而 E 是 P/Φ 的一个子域，则 P 是 E 上的正规扩张。另一方面，若 $P\supseteq E\supseteq\Phi$，则有可能出现 P/E 及 E/Φ 都是正规扩张而 P/Φ 却不是正规扩张的情况(见下面习题的第 1 题)。使

$$P=\Phi(\sigma_1,\sigma_2,\cdots,\sigma_m)$$

是 Φ 的任意有限维扩张，且 $f(x)=\Pi f_i(x)$，这里的 $f_i(x)$ 是 σ_i 在 Φ 上的最小多项式。设 Δ/P 是 $f(x)\in\Phi[x]$ 的一个分裂域，则 Δ/Φ 是 $f(x)$ 的一个分裂域，因此 Δ/Φ 是正规的。现设 Δ'/Φ 是 P/Φ 的任一正规扩张，由于 Δ' 包含 σ_i 而 $f_i(x)$ 在 Φ 中不可约，定理 8 的条件(2)表明 Δ'/Φ 包含 $f(x)$ 的一个分裂域，因此有一个 Δ/Φ 到 Δ'/Φ 内的同构，由此可推出 Δ 的包含 P 的任何真子域在 Φ 上都不是正规的。我们现在定义 P/Φ 的一个**正规闭包**为 Φ 的一个包含 P 的正规扩张，它有性质：任何包含 P 的真子域在 Φ 上都不是正规的，因此我们能够说：Δ/Φ 是 P/Φ 的一个正规闭包，而关于 Δ 及 Δ' 的附注表明这样的一个扩张在 Φ 同构的

意义下被 P/Φ 完全确定．

习　题　9

1．设 $P=R_0(\sqrt[4]{2})$，R_0 为有理数域，又设 $E=R_0(\sqrt{2})\subseteq P$．证明 P/E 及 E/R_0 是正规的但 P/R_0 却不是正规的．

9. 代数扩张的结构．可分性　域的结构理论将在第四章中详细讨论，目前宜于推导出代数扩张的基本定理及更一般的任意域 P/Φ 的代数元集的基本定理．我们在卷1(中译本 p.169)中已经证明：如果 P 是 Φ 上的一个域，则由 P 的 Φ 上的代数元组成的子集 A 作成 Φ 上的一个子域，而且 P 的每一个 A 上的代数元必包含于 A 中，子域 A/Φ 称为 Φ 在 P 中的**代数闭包**，如果 $\Phi=A$，则 Φ 称为**在 P 中为代数闭的**；若 $P=A$（即 P 的每个元都是 Φ 上的代数元），则域 P/Φ 称为**代数的**．上面引述结果的第二部分是：若 A 是 Φ 在 P 中的代数闭包，则 A 在 P 中是代数闭的．我们将给出这些结果的另一证明，这一证明基于 §5 引理 2：若 ρ_i 是 $\Phi(\rho_1,\cdots,\rho_{i-1})$ 上的代数元，则 $\Phi(\rho_1,\rho_2,\cdots,\rho_n)/\Phi$ 是有限维的．现设 A 是由 P 的 Φ 上的代数元构成的集，且设 $\rho,\sigma\in A$，则 $\Phi(\rho,\sigma)$ 是有限维的．由于对于超越元 τ，$\Phi(\tau)/\Phi$ 是无限维的，故可推得 $\Phi(\rho,\sigma)$ 的每个元都是 Φ 上的代数元．特别地，$\rho\pm\sigma$，$\rho\sigma$，及 ρ^{-1}(当 $\rho\neq 0$ 时)都是代数元．由于 ρ 与 σ 是 P 中的任意元，由此可推出 A 是 P 的一个子域，显然还有 $A\supseteq\Phi$．现设 ρ 是 P 的在 A 上的代数元且设 $f(x)=x^n+\alpha_1x^{n-1}+\cdots+\alpha_n$ 是它在 A 上的最小多项式，则 $\alpha_i\in A$，因此是 Φ 上的代数元．此外，显然 ρ 是 $\Phi(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 上的代数元，于是可得出 $\Phi(\alpha_1,\alpha_2,\cdots,\alpha_n,\rho)$ 是 Φ 上的有限维扩张域，因此 ρ 是 Φ 上的代数元，从而 A 在域 P 中是代数闭的．我们所证明的有关 P 中 A 的代数闭包的结果可推出以下传递性：**若 B/A 是代数的，且 A/Φ 是代数的，则 B/Φ 也是代数的**．为此令 Γ/Φ 是由 B/Φ 的在 Φ 上的代数元组成的子域，显然 $\Gamma\supseteq A$，我们已经看到，若 $\beta\in B$ 是 Γ 上的代数元，则它属于 Γ．另一方面，若 β 是 B 的任意元，则 β 是 A 上的代

数元，因此也是 Γ 上的代数元，故 $\beta\in\Gamma$，这表明 $B=\Gamma$ 是 Φ 上的代数扩张。

关于代数元还有几个有用的附注值得记录于此以便今后参考。其中第一个是隐含在前面我们已证明的定理中的，它是：若 $\mathfrak{A}/\Phi$ 是域 P/Φ 的一个子代数，则 $\mathfrak{A}$ 的每个元在 Φ 上都是代数的当且仅当 $\mathfrak{A}$ 的每个有限子集 X 都被包含在一个有限维子代数 $\mathfrak{X}/\Phi$ 之中，由此可推出：每个 $\xi\in\mathfrak{A}$ 都是 Φ 上的代数元，因为由它可推出 $\Phi[\xi]$ 是有限维的。另一方面，若 $\mathfrak{A}$ 的每个元都是代数的且 $X=\{\xi_1,\xi_2,\cdots,\xi_r\}$，则我们所引用的引理表明 $\Phi(\xi_1,\xi_2,\cdots,\xi_r)/\Phi$ 是有限维的。我们还要记住

$$\Phi[\xi_1,\xi_2,\cdots,\xi_r]=\Phi(\xi_1,\xi_2,\cdots,\xi_r),$$

由此推出：若 $\mathfrak{A}$ 的每个元都是代数元，则 $\mathfrak{A}$ 是 P/Φ 的一个子域。我们还应注意：若 E/Φ 是 P/Φ 的一个代数子域而 Δ/Φ 是任意一子域，则由 E 及 Δ 生成的子代数 $E\Delta/\Phi$ 是一个子域，它在 Δ 上是代数的。要弄清这点我们注意 $E\Delta$ 是形如 $\Sigma\varepsilon_i\delta_i(\varepsilon_i\in E,\delta_i\in\Delta)$ 的元的集。因此，若 X 是 $E\Delta$ 的一个有限子集，则存在一有限子集 $\{\varepsilon_i\}$，使 X 的每个元都是 ε_i 的一个 Δ 线性组合。由于 E/Φ 是代数的，因此我们可将集 $\{\varepsilon_i\}$ 嵌入一个有限维子代数。若用此子代数的一个基 $\{\eta_j\}$ 表示 ε_i，则可见 X 的每个元有形式 $\Sigma\delta_j\eta_j(\delta_j\in\Delta)$，因为 $\eta_j\eta_k=\Sigma\gamma_{jkl}\eta_l(\gamma_{jkl}\in\Phi)$，显然 η_j 的 Δ 线性组合的集 $\Sigma\Delta\eta_j$ 是 P/Δ 的一个子代数，因此我们证明了 $E\Delta$ 的每个有限子集被包含在 Δ 上的一个有限维子代数之中，因此 $E\Delta$ 的每个元都是 Δ 上的代数元，且 $E\Delta$ 是一个子域。

一代数元 $\rho\in P/\Phi$ 称为 **Φ 上的可分(代数)元**，如果它在 Φ 上的最小多项式是可分的。显然 ρ 在 Φ 上是可分的当且仅当存在一多项式 $f(x)\in\Phi[x]$，它有不同的根使 $f(\rho)=0$。还有，ρ 是可分的当且仅当存在一多项式 $f(x)\in\Phi[x]$ 使 $f(\rho)=0$ 且 $(f,f')=1$。若 Φ' 是 Φ 的一个扩张域，则在 $\Phi'[x]$ 中我们将仍有 $(f,f')=1$（这是因为 $(f,f')=af+bf'$，参考卷 1 的中译本 p.113 习题 48 的第 3 题）。由此可得，若 Φ'/Φ 是 P/Φ 的一个子域而且 $\rho\in P$

是Φ上的可分元，则ρ也是Φ'上的可分元素。我们在§6中已经看到系数在特征为0的域中的每个多项式都是可分的。因此，我们要考虑的诸结果在特征0的情况下是当然的。

扩张 P/Φ 称为(代数)可分的，如果每个元 $\rho\in P$ 是Φ上的可分元。设 Λ/Φ 是代数域，Σ是Λ的由Φ上的可分元组成的子集，我们要证明Σ是包含Φ的一个子域而且Λ的每个在Σ上的可分元必包含于Σ之中，为此需要下列结论：

引理 1. 设 $P\supseteq E\supseteq\Phi$，其中$E$及$\Phi$是$P$的子域，而且$E/\Phi$是有限维伽罗瓦扩张，则$P$的在$E$上为可分的代数元$\theta$也是$\Phi$上的可分代数元。

证 设 $g(x)$ 是θ在E上的最小多项式，若s是 E/Φ 的伽罗瓦群G的元，则s有唯一的一个到$E[x]$上的扩张满足 $x^s=x$。令 $g^{s_1}(x), g^{s_2}(x), \cdots, g^{s_r}(x)$ 是 $g(x)$ 在 $s\in G$ 下的不同的象，作 $f(x)=\prod_1^r g^{s_i}(x)$，则对于所有 $s\in G$ 有 $f^s(x)=f(x)$，由此推出$f(x)\in\Phi[x]$。由于在$E[x]$中$g(x)$是不可约的且$(g, g')=1$，这对于每个g^{s_i}也成立。因此每个 $g^{s_i}(x)$ 都有不同的根。还应注意，若 $i\neq j$，则g^{s_i}及g^{s_j}是互素的，否则 $(g^{s_i}, g^{s_j})=g^{s_i}(x)=g^{s_j}(x)$(因为它们在$E[x]$中是不可约的)，这与$i\neq j$时$g^{s_i}\neq g^{s_j}$矛盾，故 $1=(g^{s_i}, g^{s_j})$。从而在 $f(x)$ 的一个分裂域中它们没有公共根，于是显然 $f(x)$ 有相异根，由于 $f(\theta)=0$ 及 $f\in\Phi[x]$，故知θ是Φ上的可分元。

显然，若 $\rho\in E$，则ρ是E上的可分代数元(有最小多项式$x-\rho$)，因此引理1表明ρ是Φ上的可分元。换句话说，我们有

推论. 任一有限维伽罗瓦扩张都是可分的。

至此可证可分性的主要结果：

定理 11. 若 Λ/Φ 是代数扩张，则Λ的在Φ上的可分元之集Σ是一个包含Φ的子域。此外，Σ包含Λ的所有在Σ上的可分代数元。

证 设 $\rho, \sigma\in\Sigma$，$g(x)$ 及 $h(x)$ 分别是ρ及σ在Φ上的最

小多项式，则 $f(x)=g(x)h(x)$ 是可分多项式．若Δ是 $f(x)$ 在 $\Phi(\rho,\sigma)$ 上的一个分裂域，则Δ也是 $f(x)$ 在Φ上的一个分裂域（$\Phi(\rho,\sigma)/\Phi$ 的正规闭包），因此 Δ/Φ 是伽罗瓦扩张，故由上面的推论知Δ的每个元都是Φ上的可分元，特别地，$\rho\pm\sigma$，$\rho\sigma$，ρ^{-1}（当 $\rho\neq 0$ 时）及Φ的每个元都是Φ上的可分元，这就证明了Σ是包含Φ的一个子域．现设θ是A的一个在Σ上的可分代数元，而

$$x^n+\rho_1x^{n-1}+\cdots+\rho_n(\rho_i\in\Sigma)$$

是它在Σ上的最小多项式，子域 $\Phi(\rho_1,\rho_2,\cdots,\rho_n;\theta)$ 是Φ上的有限维扩张域，设 Δ/Φ 是它的正规闭包，$f_i(x)$ 是 ρ_i 在Φ上的最小多项式，则Δ包含 $f(x)=\prod_1^n f_i(x)$ 的一个分裂域 E/Φ，由于 $f(x)$ 是可分多项式，所以这个域是Φ上的伽罗瓦扩张；显然 $E\supseteq\Phi(\rho_1,\rho_2,\cdots,\rho_n)$，还有$\theta$是 $\Phi(\rho_1,\rho_2,\cdots,\rho_n)$ 上的可分元，这是因为 $x^n+\rho_1x^{n-1}+\cdots+\rho_n$ 是它的最小多项式．因此θ是E上的可分代数元，由引理1，θ是Φ上的可分代数元．这就证明了第二个论断．

若一代数扩张 A/Φ 所仅有的可分元都是Φ的元，则称 A/Φ 是**纯不可分的**．类似地，一代数元ρ是**Φ上的纯不可分元**，如果 $\Phi(\rho)/\Phi$ 是纯不可分扩张．显然由定义可得，若ρ同时是Φ上的可分元及纯不可分元，则 $\rho\in\Phi$．此外要注意的是：一元可以是不可分元（＝不是可分元）而不必是纯不可分元（请参阅下面的习题的第3题）．若 A/Φ 是代数的，Σ/Φ 是 A/Φ 的极大可分子域（即所有可分元的子域），则定理11的第二部分断言 A/Σ 是纯不可分的． 这表明每个代数扩张 A/Φ 可由两个“纯”步骤组成：第一步是作出一个可分扩张 Σ/Φ，第二步作一纯不可分扩张 A/Σ． 定理11的第二部分及本节开始时用到的有关代数扩张的判断可推出传递性： 若 A/Φ 及 B/A 都是可分代数扩张，则 B/Φ也是可分代数扩张．我们现在来证明一个有关纯不可分扩张的类似的传递性：由于上列结论在特征为0的域中是当然的，因此我们将在本节的其余部分研究特征为 $p\neq 0$ 的域，我们需要以

下的关于可分元及纯不可分元的重要判定法:

引理 2. 设 Φ 是特征为 $p \neq 0$ 的域. (i) 一扩张域的代数元 ρ 是 Φ 上的可分元当且仅当 $\Phi(\rho) = \Phi(\rho^p) = \Phi(\rho^{p^2}) = \cdots$. (ii) 若 ρ 是纯不可分元，则其最小多项式有形式 $x^{p^e} - \alpha(\alpha \in \Phi)$; 反之,若 ρ 满足作 $x^{p^e} = \alpha \in \Phi(e > 0)$ 形的方程，则 ρ 是 Φ 上的纯不可分元.

证　设 $g(x)$ 是 ρ 在 Φ 上的最小多项式. (i) 首先假设 ρ 不是可分元,则 $g(x) = h(x^p)$ 且 ρ^p 是 $h(x)$ 的一个根,因此

$$[\Phi(\rho^p):\Phi] \leqslant \deg h(x) < \deg g(x) = [\Phi(\rho):\Phi],$$

故 $\Phi(\rho^p) \subset \Phi(\rho)$. 其次假设 ρ 是可分元,故 $g(x)$ 有不同的根,设 $h(x)$ 是 ρ 在 $\Phi(\rho^p)$ 上的最小多项式,则 $h(x) | g(x)$, 所以 $h(x)$ 有不同的根,但 ρ 也是多项式 $x^p - \rho^p \in \Phi(\rho^p)[x]$ 的一个根,因此 $h(x) | x^p - \rho^p = (x - \rho)^p$. 由于 $h(x)$ 有不同的根，这可推出 $h(x) = x - \rho$, 因此 $\rho \in \Phi(\rho^p) = \Phi[\rho^p]$, 而且 ρ 是 ρ^p 的一个系数在 Φ 中的多项式，取 p 次幂后得 ρ^p 是 ρ^{p^2} 的一个系数在 Φ 的多项式,故 $\rho \in \Phi(\rho^{p^2})$, 重复这种步骤得

$$\Phi(\rho) = \Phi(\rho^p) = \Phi(\rho^{p^2}) = \cdots.$$

这就证明了 (i). (ii) 设 ρ 是 Φ 上的纯不可分元且写成 $g(x) = h(x^{p^e})$, 这里 e 是满足这式的最大数,则 $h'(x) \neq 0$, 因若不然将有 $h(x) = k(x^p)$ 及 $g(x) = k(x^{p^{e+1}})$, 这与 e 的选择矛盾,我们有 $h(\rho^{p^e}) = 0$, 故 ρ^{p^e} 是一可分多项式的根，由于假设 ρ 是纯不可分的，故推出 $\rho^{p^e} = \alpha \in \Phi$ 且 ρ 是 $x^{p^e} - \alpha$ 的一个根，由于 $g(x) = h(x^{p^e})$ 是 ρ 在 Φ 上的最小多项式,显然 $g(x) = x^{p^e} - \alpha$. 次设对于某个非负整数 e, $\rho^{p^e} = \alpha \in \Phi$, 设 $\sigma \in \Phi(\rho) = \Phi[\rho]$, 故 $\sigma = \alpha_0 + \alpha_1\rho + \cdots + \alpha_m\rho^m(\alpha_i \in \Phi)$, 所以

$$\sigma^{p^e} = \alpha_0^{p^e} + \alpha_1^{p^e}\rho^{p^e} + \cdots + \alpha_m^{p^e}(\rho^{p^e})^m \in \Phi.$$

若 σ 是可分元,则由 (i) 有 $\Phi(\sigma) = \Phi(\sigma^{p^e})$, 因此 $\Phi(\sigma) = \Phi$ 及 $\sigma \in \Phi$, 故 ρ 是纯不可分元.

这个引理的第二部分表明 A/Φ 是纯不可分扩张当且仅当 A 的每个元满足方程 $x^{p^e} = \alpha \in \Phi$, 由于 $(x^{p^e})^{p^f} = x^{p^{e+f}}$, 这可推

出：若 B/A 及 A/Φ 都是纯不可分扩张，则 B/Φ 也是纯不可分扩张．由引理的第二部分还可见：若 A 在 Φ 上是纯不可分的，则它在 P/Φ 的任一子域 E 上都是纯不可分的．

习　题　10

1.设 A/Φ 是代数扩张，验证 A 的在 Φ 上为纯不可分的元 r 的集组成包含 Φ 的一个子域．

2.设 I_p 是域 $I/(p)$，$\mathrm{P} = I_p(\xi, \eta)$，这里 ξ, η 是未定元（参考§6习题的第3题），设 $\Phi = I_p(\xi^p, \eta^p - \eta - \xi)$．证明 $[\mathrm{P}:\Phi] = p^2$ 并确定 P/Φ 的极大可分子域．

3.（J. D. 莱特（Reid））P如第2题所示，$E = \mathrm{P}(\zeta)$，这里 $\zeta^{p^2} = \xi\zeta^p + \xi\eta$．证明 $[E:\mathrm{P}] = p^2$ 且 E/P 是不可分扩张域，并证 E/P 不能包含不属于P的P上的纯不可分元．

4.设 P/Φ 是代数扩张，$\mathrm{P}(\xi_1, \xi_2, \cdots, \xi_r)$ 是 $\mathrm{P}[\xi_1, \xi_2, \cdots, \xi_r]$ 的分式域，ξ_i 是未定元，A 是 $\mathrm{P}(\xi_r)$ 中形如 Fg^{-1} 的元的集，这里 $F \in \mathrm{P}[\xi_1, \cdots, \xi_r]$，$g \in \Phi[\xi_1, \cdots, \xi_r]$．证明 A 是 $\mathrm{P}(\xi_1, \cdots, \xi_r)/\Phi(\xi_1, \cdots, \xi_r)$ 的一个子域，它是代数的．再证 $A = \mathrm{P}(\xi_1, \cdots, \xi_r)$，从而每个系数在P中的非零多项式有一个系数在 Φ 中的非零倍式．

10. 可分次数与不可分次数．　正规扩张的结构　我们在本节讨论的域均假定是特征 $p \neq 0$ 的，并且考虑的是有限维扩张．对于这样的具有极大可分子域 Σ/Φ 的一个扩张 P/Φ 我们考虑维数 $[\Sigma:\Phi]$ 及 $[\mathrm{P}:\Sigma]$，它们分别称为 P/Φ 的**可分次数**及**不可分次数**，并写成 $[\Sigma:\Phi] = [\mathrm{P}:\Phi]_s$，$[\mathrm{P}:\Sigma] = [\mathrm{P}:\Phi]_i$，那么我们有

$$[\mathrm{P}:\Phi] = [\mathrm{P}:\Phi]_s[\mathrm{P}:\Phi]_i. \tag{11}$$

我们现在证明 $[\mathrm{P}:\Phi]_i = p^f$，这就是说一个纯不可分扩张的维数是其特征的一个方幂：若 $\mathrm{P} = \Phi$，这是显然的，因为 $[\mathrm{P}:\Phi] = 1 = p^0$；否则设 $\rho \in \mathrm{P}$，但 $\rho \notin \Phi$，则§9引理2表明，ρ 在 Φ 上的最小多项式有次数 $p^e(e > 0)$，故 $[\Phi(\rho):\Phi] = p^e$ 而且 $[\mathrm{P}:\Phi(\rho)] < [\mathrm{P}:\Phi]$．由于P是 $\Phi(\rho)$ 上的纯不可分扩域，我们可（对维数作归纳）假设 $[\mathrm{P}:\Phi(\rho)] = p^g$，从而 $[\mathrm{P}:\Phi] = p^e p^g = p^{e+g}$．

我们现在考虑接连的两个有限维扩张：设 Δ/P 是有限维扩张而且 P/Φ 也是有限维扩张，则 Δ/Φ 是有限维扩张；我们已经看到，若 P/Φ 及 Δ/P 都是可分（纯不可分）扩张，则 Δ/Φ 也是可分（纯不可分）扩张；若 P/Φ 是可分的而 Δ/P 是纯不可分的，

则易见 P/Φ 是 Δ/Φ 的极大可分子域，因此 $[\Delta:\Phi]_s=[P:\Phi]_s$，而 $[\Delta:\Phi]_i=[\Delta:P]$。现在再考虑它们的有趣的搭配：设 P/Φ 是纯不可分的，Δ/P 是可分的，我们将证明最后的 Δ/Φ 的极大可分子域与 Δ/P 有相同的维数，一个较简短的命题是如下。

引理. 设 Δ/P 是可分的，P/Φ 是纯不可分的，则 $\Delta/\Phi=P\otimes_\Phi\Sigma$，这里的 Σ/Φ 是 Δ/Φ 的极大可分子域，而且

$$[\Delta:P]=[\Sigma:\Phi]$$

证 从导言中的 XII 易见命题 $\Delta=P\otimes_\Phi\Sigma$ 等价于：存在 Σ 的一个 Φ 基，它同时又是 Δ 的一个 P 基，这就可得到 $[\Sigma:\Phi]=[\Delta:P]$。现在来确定这个基的形式：首先，设 $(\delta_1,\delta_2,\cdots,\delta_n)$ 是 Δ/P 的一个基，写出 $\delta_i\delta_j=\sum_k\rho_{ijk}\delta_k$，$\rho_{ijk}\in P$。若 δ 是 Δ 的任一元，$g(x)=h(x^{p^e})$ 是它在 Φ 上的最小多项式，而 $h(x)$ 是可分多项式，则 δ^{p^e} 在 Φ 上是可分的，因此 $\delta^{p^{e+f}}=(\delta^{p^e})^{p^f}$ 也是可分的。由此推得：我们可选取 e 使每个 $\delta_i^{p^e}$ 及每个 $\rho_{ijk}^{p^e}$ 是 Φ 上的可分元。由于 P/Φ 是纯不可分的，由它可得 $\alpha_{ijk}=\rho_{ijk}^{p^e}\in\Phi$，我们有 $\delta_i^{p^e}\delta_j^{p^e}=\Sigma\rho_{ijk}^{p^e}\delta_k^{p^e}$，因此若令 $\delta_i^{p^e}=\sigma_i$，则有 $\sigma_i\in\Sigma$ 及 $\sigma_i\sigma_j=\Sigma\alpha_{ijk}\sigma_k$，$\alpha_{ijk}\in\Phi$。我们说 $(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 是 Δ/P、同时又是 Σ/Φ 的一个基。我们首先由 σ_i 的乘法表可以看出 $\sum_i\Phi\sigma_i$ 是 Σ/Φ 的一个 Φ 子代数，而 $\sum_i P\sigma_i$ 是 Δ/P 的一个 P 子代数。又 σ_i 的个数也是 n，因此要证明 $(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 是 Δ 的一个 P 基，只要证明每个 $\delta\in\Delta$ 是 σ_i 的一个 P 线性组合就行了；要证明 $(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 是 Σ 的一个 Φ 基也只要证明每个 $\sigma\in\Sigma$ 是 σ_i 的一个 Φ 线性组合就行了。这是因为：若它们是 P 线性无关的，则它们必定是 Φ 线性无关的。现设 $\delta\in\Delta$，则 δ 是 P 上的可分元素，因此 $\delta\in P[\delta^{p^e}]$。我们有 $\delta=\Sigma\rho_i\delta_i(\rho_i\in P)$，这是因为 $(\delta_1,\cdots,\delta_n)$ 是一个 P 基。因此

$$\delta^{p^e}=\Sigma\rho_i^{p^e}\delta_i^{p^e}=\Sigma\rho_i^{p^e}\sigma_i\in\Sigma P\sigma_i.$$

由于 $\delta\in P[\delta^{p^e}]$，这可推出 $\delta\in\sum_i P\sigma_i$。次设 $\sigma\in\Sigma$，则如刚才所

证，$\sigma=\sum\rho_i\sigma_i(\rho_i\in P)$。若 f 足够大，则

$$\rho_i^{p^f}\in\Phi,\ \sigma^{p^f}=\sum\rho_i^{p^f}\sigma_i^{p^f}\in\sum_i\Phi\sigma_i.$$

由于 σ 是 Φ 上可分元，$\sigma\in\Phi[\sigma^{p^f}]\subseteq\sum_i\Phi\sigma_i$。证毕。

我们现在可以证明

定理 12. 若 Δ/P 及 P/Φ 都是有限维扩域，则

(12) $[\Delta:\Phi]_s=[\Delta:P]_s[P:\Phi]_s, [\Delta:\Phi]_i=[\Delta:P]_i[P:\Phi]_i$.

证 只须证明第一个等式就够了，因为第二个可由它及(11)推得。首先设 Δ/P 是纯不可分的，则 Δ/Φ 的在 Φ 上可分的任一元都是在 P 上可分的，从而属于 P。故 Δ/Φ 的极大可分子域 Σ/Φ 必包含于 P 中，它是 P/Φ 的极大可分子域，因此 $[\Delta:\Phi]_s=[P:\Phi]_s$。另一方面，因 Δ/P 是纯不可分的，$[\Delta:P]_s=1$，因此在此情况下(12)成立。次设 Δ/P 是可分扩张域，将 P/Φ 的极大可分子域 Σ/Φ 作为基域考虑，在可分扩张 Δ/P 及纯不可分扩张 P/Σ 上应用引理可得 $[\Delta:P]=[\Sigma':\Sigma]$，这里 Σ'/Σ 是 Δ/Σ 的极大可分子域。由于可分性是传递的，显然 Σ'/Φ 是 Δ/Φ 的极大可分子域，因此，由定义 $[\Delta:\Phi]_s=[\Sigma':\Phi]$，且

$$[\Delta:\Phi]_s=[\Sigma':\Phi]=[\Sigma':\Sigma][\Sigma:\Phi]=[\Delta:P][\Sigma:\Phi].$$

显然，$[\Sigma:\Phi]=[P:\Phi]_s$，而且由于 Δ/P 是可分的，$[\Delta:P]=[\Delta:P]_s$，将它代入上等式就可得到等式(12)。故在这种情况下，(12)是成立的。最后设 Δ/P 是任意的，E/P 是 Δ/P 的极大可分子域，则 Δ/E 是纯不可分的。然后考虑 $E\supseteq P\supseteq\Phi$（这里 E/P 是可分的）我们就可见 $[E:\Phi]_s=[E:P]_s[P:\Phi]_s$。由于 Δ/E 是纯不可分的，将第一种情况应用到 $\Delta\supseteq E\supseteq\Phi$ 可得 $[\Delta:\Phi]_s=[\Delta:E]_s[E:\Phi]_s$。同理，若考虑 $\Delta\supseteq E\supseteq P$，则可得 $[\Delta:P]_s=[\Delta:E]_s[E:P]_s$。将它们联合起来，可得

$$\begin{aligned}[\Delta:\Phi]_s&=[\Delta:E]_s[E:\Phi]_s\\&=[\Delta:E]_s[E:P]_s[P:\Phi]_s\\&=[\Delta:P]_s[P:\Phi]_s,\end{aligned}$$

这就是在一般情况下的(12).

我们已经看到,若 P/Φ 是伽罗瓦扩张,则 P/Φ 是可分的(§9 引理 1 推论);又由于 P/Φ 是一个分裂域,所以这个扩张是正规的. 反之,若 P/Φ 是正规的及可分的,则 P/Φ 是一个可分多项式的分裂域,因此 P/Φ 是伽罗瓦扩张. 所以条件"P/Φ 是伽罗瓦扩张"等价于"P/Φ 是可分的及正规的扩张." 我们还要指出的是:任一纯不可分扩张 P/Φ 都是正规扩张. 要证明它可对 $\sigma\in P$ 取不可约多项式 $g(x)\in \Phi[x]$ 且设 $g(\sigma)=0$,则 $g(x)$ 是 σ 在 Φ 上的最小多项式,故 $g(x)=x^{p^e}-\alpha$. 由于 $\sigma^{p^e}=\alpha$,我们有分解 $g(x)=x^{p^e}-\alpha=x^{p^e}-\sigma^{p^e}=(x-\sigma)^{p^e}$,故 $g(x)$ 是 $P[x]$ 中的线性因子的乘积,从而 P/Φ 是正规的. 下列定理给出正规扩张结构的一个颇为精确的描述:

定理 13. 若 P/Φ 是有限维正规扩张,则 $P=\Sigma\otimes_\Phi\Gamma$,这里 Σ/Φ 是伽罗瓦扩张,而 Γ/Φ 是纯不可分扩张. 反之,若 Γ/Φ 是一个有限维纯不可分扩张,Σ/Φ 是有限维可分扩张,则代数 $P/\Phi=\Gamma\otimes_\Phi\Sigma$ 是一个域而且当 Σ/Φ 是伽罗瓦扩张时是一个正规扩张.

证 假设 P/Φ 是一个有限维正规扩张,令 Γ 为 Φ 上纯不可分元的集,则 Γ 是 Φ 上的一个子域(§9 习题中的第 1 题). 设 $\rho\in P$ 及 $g(x)$ 是 ρ 在 Φ 上的最小多项式,$g(x)=h(x^{p^e})$,这里 $h(x)$ 是可分多项式. 由于 $g(x)$ 在 $\Phi[x]$ 中是不可约的,显然 $h(x)$ 在 $\Phi[x]$ 中也是不可约的. 因为 $h(\rho^{p^e})=0$,由 P/Φ 的正规性可推出:在 $P[x]$ 中 $h(x)=\prod_1^r(x-\beta_i)$. 再有

$$g(x)=h(x^{p^e})=\prod_1^r(x^{p^e}-\beta_i)$$

在 $P[x]$ 中也是线性因子的一个乘积,因此 $x^{p^e}-\beta_i$ 有一根 ρ_i 在 P 中,从而 $x^{p^e}-\beta_i=x^{p^e}-\rho_i^{p^e}=(x-\rho_i)^{p^e}$,故

$$g(x)=h(x^{p^e})=\prod_1^r(x^{p^e}-\beta_i)=\prod_1^r(x-\rho_i)^{p^e}.$$

现使 $k(x)=\prod_{1}^{r}(x-\rho_i)$，由于 $\beta_i=\rho_i^{p^e}$ 是相异的，所以各 ρ_i 也是相异的，我们有 $k(x)^{p^e}=\Pi(x^{p^e}-\rho_i^{p^e})=\Pi(x^{p^e}-\beta_i)=g(x)$，若 $k(x)=x^m+\sigma_1x^{m-1}+\cdots+\sigma_m$，则 $\sigma_i\in P$，

$$k(x)^{p^e}=x^{mp^e}+\sigma_1^{p^e}x^{(m-1)p^e}+\cdots+\sigma_m^{p^e}=g(x);$$

这表明 $\sigma_i^{p^e}\in\Phi$，故 $\sigma_i\in\Gamma$，而 $k(x)\in\Gamma[x]$. 由于 ρ 是 $k(x)$ 的一个根且 $k(x)$ 的根相异，故 ρ 是 Γ 上的可分元. 由于 ρ 是 P 的任意元，这就证明了 P/Γ 是可分的，由本节开始时的引理可得分解 $P=\Gamma\otimes_\Phi\Sigma$，这里的 Σ 是 P/Φ 的极大可分子域. 若 $\sigma\in\Sigma$ 且 $f(x)$ 是它在 Φ 上的最小多项式，则在 $P[x]$ 中 $f(x)=\Pi(x-\sigma_k)$. 显然各 σ_k 在 Φ 上是可分的，所以它们包含于 Σ 中，因此分解

$$f(x)=\Pi(x-\sigma_k)$$

在 $\Sigma[x]$ 中成立，这就证明了 Σ/Φ 是正规的及可分的，故是 Φ 上的伽罗瓦扩张. 第一个命题至此证完. 现设 P/Φ 是有限维纯不可分扩张而 Σ/Φ 是有限维可分扩张，我们将首先指出：若 $(\sigma_1,\sigma_2,\cdots,\sigma_m)$ 是 Σ/Φ 的一个基，则 $(\sigma_1^{p^e},\sigma_2^{p^e},\cdots,\sigma_m^{p^e})$ $(e\geqslant1)$ 也是. 显然这只要证明每个元 $\sigma\in\Sigma$ 是各 $\sigma_i^{p^e}$ 的一个 Φ 线性组合就行了. 我们知道，对于任何 $j\geqslant0$，σ^j 是 σ_i 的一个线性组合；取 p^e 次方幂后得 $(\sigma^{p^e})^j$ 是 $\sigma_i^{p^e}$ 的一个 Φ 线性组合，这里 $j=0,1,2,\cdots$，由于 σ 是可分的，可知 $\sigma\in\Phi[\sigma^{p^e}]$ (§9 引理 2)，因此 $\sigma\in\sum_i\Phi\sigma_i^{p^e}$，而 $(\sigma_1^{p^e},\sigma_2^{p^e},\cdots,\sigma_m^{p^e})$ 是 Σ/Φ 的一个基. 现考虑 $P=\Gamma\otimes_\Phi\Sigma$，这是一个交换代数，它的任意元均可写成 $\Sigma\gamma_i\otimes\sigma_i$ 的形式，这里 $\gamma_i\in\Gamma$，$(\sigma_1,\cdots,\sigma_m)$ 则是 Σ/Φ 的基. 今若 $\rho=\Sigma\gamma_i\otimes\sigma_i\neq0$，则有一个 γ_i (不妨设为 γ_1) $\neq0$，由于 Γ/Φ 是纯不可分的，我们可选取 $e\geqslant0$ 使 $\gamma_i^{p^e}=\alpha_i\in\Phi$ $(1\leqslant i\leqslant m)$，故有 $\rho^{p^e}=\Sigma\alpha_i\otimes\sigma_i^{p^e}=1\otimes\Sigma\alpha_i\sigma_i^{p^e}$，由于 $(\sigma_1^{p^e},\cdots,\sigma_m^{p^e})$ 是 Σ/Φ 的一个基，$\alpha_1\neq0$，$\Sigma\alpha_i\sigma_i^{p^e}$ 是 Σ 的一个非零元. 由于它在 Σ 中有一逆元，故 ρ 在 P 中有一逆元，故 P 是一个域. 现设 Σ/Φ 是伽罗瓦扩域，则 Σ/Φ 是一多项式 $g(x)\in\Phi[x]$ 的一个分裂域且 Γ/Φ

是 $h(x)\in\Phi[x]$ 的一个分裂域，由于 P 是由与 Γ 及 Σ 同构的子域生成的，故推得 P/Φ 是 $g(x)h(x)$ 的一个分裂域，从而 P/Φ 是正规扩张。

习　题　11

1. 设 E/Φ 为有限维域扩张，P/Φ 为任意域扩张，证明：E/Φ 到 P/Φ 内的不同的同构的个数不超过 $[E:\Phi]_s$。证明：在 P/Φ 是 E/Φ 的正规闭包时方能等于此数。

2. 设 P/Φ 是有限维正规扩域，Σ/Φ 是极大可分子域，G 是 P/Φ 的伽罗瓦群，证明 G 将 Σ 映入其本身内，而且映射 $S\to\bar{S}$ 是 G 到 Σ/Φ 的伽罗瓦群上的一个同构，这里 $\bar{S}$ 是 $S\in G$ 在 Σ 上的限制。再证 $I(G)=\Gamma/\Phi$，这里 Γ/Φ 是 P/Φ 的极大纯不可分子域。

11. 本原元　我们将在本节及下节得到有限维扩张域 P/Φ 的某些特殊生成法，这些结果对任意的 Φ 都是有效的；但是这两节的证明需要 Φ 是无限域，对于有限域 Φ 此结果的有效性将在 §13 中建立。

若 $P=\Phi(\theta)$，即 P 是在 Φ 上由 θ 生成的域，我们曾称 P 是 Φ 的一个单扩张(见卷 1 的中译本 p.94) 我们现在将称 θ 是 P/Φ 的一个本原元，并将证明本原元的存在性的两个结果。

定理 14.　设 Φ 是一个无限域，$P=\Phi(\xi,\eta)$ 是一个在 Φ 上由一个可分代数元 ξ 及一个代数元 η 生成的域，则 P/Φ 必有一本原元。

证　设 $f(x)$ 及 $g(x)$ 分别是 ξ 及 η 在 Φ 上的最小多项式，Δ/P 是 $f(x)g(x)$ 的一个分裂域，则 Δ/Φ 是 $f(x)g(x)$ 的包含 P 的一个分裂域。使 $\xi_1=\xi_1,\xi_2,\cdots\xi_m$ 是 $f(x)$ 的不同的根，而 $\eta_1,\eta_2,\cdots,\eta_r$ 是 $g(x)$ 的，则这些 ξ_i 是 $f(x)$ 的全部根，我们可假设 $m>1$ (否则 $\xi\in\Phi$ 而 $P=\Phi(\eta)$)，现考虑线性方程组 $x\xi_1+\eta_1=x\xi_i+\eta_j(i=2,\cdots,m;j=1,\cdots,r)$ 中的一个，在 Φ 中它最多只有一个解。由于 Φ 是无限域，我们必能避开这些方程的解的有限集而选取 $x=\gamma\in\Phi$ 使 $\gamma\xi_1+\eta_1\neq\gamma\xi_i+\eta_j(i=2,\cdots,m;j=1,\cdots,r)$。我们断言 $\theta=\gamma\xi_1+\eta_1$ 是 P 的一个本原元。为此可考虑多项式 $g(\theta-\gamma x)$，它显然属于 $\Phi(\theta)[x]$。我们有 $g(\theta-\gamma\xi_1)=g(\eta_1)=0$ 及 $g(\theta-\gamma\xi_i)\neq0$，后者是因为

$\theta - \gamma\xi_i \neq \eta_j (i = 2, \cdots, m;\ j = 1, 2, \cdots r)$ 的缘故. 因此

$$g(\theta - \gamma x) \text{ 与 } f(x) = \prod_{1}^{m} (x - \xi_i)$$

的最高公因子是 $x - \xi = x - \xi_1$, 故存在 $A(x), B(x) \in \Phi(\theta)[x]$ 使 $(x - \xi) = A(x)f(x) + B(x)g(\theta - \gamma x)$, 故 $\xi \in \Phi(\theta)$, 因而 $\eta = \theta - \gamma\xi \in \Phi(\theta)$, 而 θ 是一个本原元.

对 k 作归纳, 这一结果可立即推广为: 若 $\mathrm{P} = \Phi(\xi_1, \cdots, \xi_k, \eta)$, 这里 ξ_i 是可分代数元而 η 是代数元, 则 P 必有一本原元. 特别地, 任一有限维可分扩张域有一本原元. 我们应注意这样的一个扩张域的中间域的个数是有限的, 这是因为 P 能嵌入于一个有限维伽罗瓦扩张 Δ/Φ 之中, Δ 与 Φ 之间的中间域的集是与 Δ/Φ 的伽罗瓦群这一有限群的子群集成 1—1 对应的. 因此关于有限维可分扩张的本原元的定理是下列定理的结果:

定理 15 (阿廷) 设 Φ 是一个无限域, 而 P 是 Φ 的一个有限维扩张域, 则 P/Φ 是一个单扩张当且仅当在 P 与 Φ 之间仅有有限多个中间域.

证 首先假设 $\mathrm{P} = \Phi(\theta)$ 而 E 是一个中间域, 令 $g(x)$ 是 θ 在 E 上的最小多项式而 E'/Φ 是由 $g(x)$ 的系数生成的域, 则 $E' \subseteq E$; 但 $g(x)$ 也是 θ 在 E' 上的最小多项式, 因此 $[\mathrm{P}:E'] = \deg g(x) = [\mathrm{P}:E]$, 故 $E = E'$ 是由 $g(x)$ 的系数生成的. 今 $g(x)$ 是 θ 在 Φ 上的最小多项式 $f(x)$ 的一个因子且 $g(x)$ 与 $f(x)$ 二者都属于 $\mathrm{P}[x]$, 由于 $f(x)$ 在 $\mathrm{P}[x]$ 中仅有有限多个首项系数为 1 的不同因子, 故 E 的个数是有限的. 次设在 P 与 Φ 间仅有有限多个中间域, 我们只须证明, 若 $\xi, \eta \in \mathrm{P}$, 则 $\Phi(\xi, \eta)$ 是单扩张就行了. 现设 $\alpha \in \Phi$ 并考虑子域 $\mathrm{P}_\alpha = \Phi(\xi + \alpha\eta)$, 我们有无限多个 $\alpha \in \Phi$ 及有限多个 P_α, 故在 Φ 中存在 $\alpha, \beta (\alpha \neq \beta)$ 使 $\mathrm{P}_\alpha = \mathrm{P}_\beta$, 则 $\eta = (\alpha - \beta)^{-1}(\xi + \alpha\eta - \xi - \beta\eta) \in \mathrm{P}_\alpha$, 故 $\xi = \xi + \alpha\eta - \alpha\eta \in \mathrm{P}_\alpha$, 因此 $\mathrm{P}_\alpha = \Phi(\xi, \eta)$, 而这是由 $\xi + \alpha\eta$ 生成的.

习　题　12

1. 设 Φ_0 是特征 $p\neq 0$ 的域，$P=\Phi_0(\xi,\eta)$ 是 $\Phi[\xi,\eta]$ 的分式域，这里 ξ,η 是未定元，$\Phi=\Phi_0(P^p)$ 是所有 p 次幂在 Φ_0 上生成的子域. 证明 $[P:\Phi]=p^2$，而且 P 没有 Φ 上的本原元.

2. 设 P 是 $(x^2-3)(x^2-2)$ 在有理数域上的分裂域，试找 P 的一个本原元.

3. 题如上，但多项式是 x^3-2.

12. 正规基　若 P 是 Φ 上的有限维伽罗瓦扩张，其伽罗瓦群 $G=\{s_1,s_2,\cdots,s_n\}$，则 $\rho\in P$ 在 Φ 上有一个次数为 n 的最小多项式当且仅当各 $\rho^{s_i}(i=1,\cdots,n)$ 是互异的. 这是很明显的，因为如果 $\rho^{s_1},\cdots,\rho^{s_r}$ 是互异的共轭元，则

$$f(x)=\prod_{j=1}^{r}(x-\rho^{s_j})$$

是 ρ 在 Φ 上的最小多项式. 还可见 ρ 是 P/Φ 的一个本原元当且仅当其最小多项式的次数 $n=(G:1)$. 因此 ρ 是一个本原元当且仅当各 $\rho^{s_i}(i=1,2,\cdots,n)$ 是互异的. 比这个更强的条件显然是这些元是线性无关的，这时我们有 P 在 Φ 上的基

$$(\rho^{s_1},\rho^{s_2},\cdots,\rho^{s_n}),$$

这种由单独元的各共轭元构成的基称为该伽罗瓦扩张的**正规基**. 我们要在这里证明这样的基，当 Φ 是无穷域时它一定存在，这事实的证明基于同构的代数无关这个概念上，这一概念本身就很重要. 我们如下给出.

定义 2　设 E 是 Φ 上的一个域，Ω 是 E 的一个扩张域，设 $s_1,\cdots,s_m$ 是 E/Φ 到 Ω/Φ 内的同构，则称 s_i 在 Ω 上是代数无关的，如果以下条件成立：使 $f(x_1,x_2,\cdots,x_m)\in\Omega[x_1,x_2,\cdots,x_m]$（这里 x_i 是未定元）对于一切 $\eta\in E$ 都有 $f(\eta^{s_1},\eta^{s_2},\cdots,\eta^{s_m})=0$ 的多项式只有 $f=0$ 一个.

我们需要以下结论

引理.　设 Ω 是一个无限域 Φ 的扩张域，

$$f(x_1,\cdots,x_m)\in\Omega[x_1,\cdots,x_m],$$

它对于一切 $\xi_i\in\Phi$ 都有 $f(\xi_1,\cdots,\xi_m)=0$，则 $f=0$.

证　设 (ω_a) 是Ω在Φ上的一个基，则可写成

$$f(x_1,\cdots,x_m)=\sum_1^r f_j(x_1,\cdots,x_m)\omega_j,$$

这里 $\{\omega_j\}$ 是 (ω_a) 的一个有限子集而 $f_j\in\Phi[x_1,\cdots,x_m]$，则 $0=f(\xi_1,\cdots,\xi_m)=\Sigma f_j(\xi_1,\cdots,\xi_m)\omega_j$ 对一切 $\xi_i\in\Phi$ 成立。由于各 ω_j 是Φ无关的，而且 $f_j(\xi_1,\cdots,\xi_m)\in\Phi$，由此推出每个 $f_j(\xi_1,\cdots,\xi_m)=0$。由卷1的中译本 p.104 所证的结果得 $f_j(x_1,\cdots,x_m)=0$，对一切 j 成立，故 $f(x_1,\cdots,x_m)=0$。

现在可以证明下面关于同构的代数无关定理：

定理 16. 设 P 是一无限域Φ上的有限维伽罗瓦扩张，E是 P/Φ 的一个子域，Ω是P的任一扩张域，令 $s_1,s_2,\cdots,s_m$ 是（Φ上的）E到（Φ上的）P内的不同的同构，则各 s_i 在Ω上代数无关。

证　我们知道同构个数 $m=[E:\Phi]$(§7)。其次，若 $(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_m)$ 是 E/Φ 的一个基，则 (i,j) 元素是 $\varepsilon_i^{s_j}$ 的矩阵的行列式 $\det(\varepsilon_i^{s_j})$ 不为0（否则此矩阵的各行是P相关的），故在Φ中存在不全为0的 ρ_j 使 $\Sigma\rho_j\varepsilon_i^{s_j}=0(i=1,2,\cdots,m)$。若$\varepsilon$是$E$的任意元素，则我们可写成 $\varepsilon=\Sigma\beta_i\varepsilon_i(\beta_i\in\Phi)$，代人后可得 $\sum_{i,j}\beta_i\rho_j\varepsilon_i^{s_j}=0$，由于 $\beta_i^{s_j}=\beta_i$，我们有 $\sum_j\rho_j\varepsilon^{s_j}=0$。这表明算子 $\Sigma s_j\rho_jR=0$，与同构的戴得金无关定理矛盾，这就证明了 $\det(\varepsilon_i^{s_j})\neq0$。现假设 $f\in\Omega[x_1,x_2\cdots,x_m]$ 且对一切 $\varepsilon\in E$ 都有 $f(\varepsilon^{s_1},\varepsilon^{s_2},\cdots,\varepsilon^{s_m})=0$，则对无限域$\Phi$的一切 β_i 也有

$$f(\Sigma\beta_i\varepsilon_i^{s_1},\Sigma\beta_i\varepsilon_i^{s_2},\cdots,\Sigma\beta_i\varepsilon_i^{s_m})=0,$$

现设

$g(x_1,\cdots,x_m)=f(\Sigma x_i\varepsilon_i^{s_1},\Sigma x_i\varepsilon_i^{s_2},\cdots,\Sigma x_i\varepsilon_i^{s_m})\in\Omega[x_1,\cdots,x_m]$，它对于所有的 $x_i=\beta_i\in\Phi$ 都等于零，故由引理 $g(x_1,\cdots,x_m)=0$。令 $\det(\varepsilon_i^{s_j})\neq0$，故矩阵 $(\varepsilon_i^{s_j})$ 有一逆 (μ_{ij})，于是

$$f(x_1,\cdots,x_m)=g(\Sigma x_j\mu_{j1},\Sigma x_j\mu_{j2},\cdots,\Sigma x_j\mu_{jn})=0.$$

这就证明了 $s_1,\cdots,s_m$ 是在Ω上代数无关的。

利用这个结果可证

定理 17. 设 P 是一无限域 Φ 上的有限维伽罗瓦扩张，则 P/Φ 有一个正规基.

证 设 $G=\{s_1,\cdots,s_n\}$ 是 P/Φ 的伽罗瓦群，我们刚才已经看到，若 $(\rho_1,\cdots,\rho_n)$ 是 P 在 Φ 上的一个基，则 $\det(\rho_i^{s_j})\neq 0$。反之，这也是构成一个基的充分条件，因为如果 $\Sigma\beta_i\rho_i=0(\beta_i\in\Phi)$，则 $\Sigma\beta_i\rho_i^{s_j}=0(j=1,2,\cdots m)$，故矩阵 $(\rho_i^{s_j})$ 的各列是 Φ 相关的(除非每个 $\beta_i=0$)。这判别法表明：对一特殊的 ρ 来说，$(\rho^{s_1},\rho^{s_2},\cdots,\rho^{s_n})$ 是一个正规基当且仅当 $\det(\rho^{s_i s_j})\neq 0$. 我们改写为 $s_i s_j=s_{i_j}$，则 $(1_j,2_j,\cdots,n_j)$ 是 $(1,2,\cdots,n)$ 的一个排列。今考虑 (i,j) 元是 $P[x_1,\cdots,x_n]$ 中的未定元 $x_{i_j}(i_j=1,2,\cdots n)$ 的矩阵，我们可断言多项式 $d(x_1\cdots,x_n)=\det(x_{i_j})\neq 0$. 为此可特取 $x_1=1$, $x_2=\cdots=x_n=0$，由于 (x_{i_j}) 的每行和每列恰好包含一个 x_1，如果如上限定各 x_i，则 $\det(x_{i_j})=\pm 1$，故 $d(x_1,\cdots,x_n)\neq 0$，因而由 x_i 的代数无关性我们可找得一个 $\rho\in P$ 使 $\det(\rho^{s_i s_j})=\det(\rho^{s_{i_j}})\neq 0$，从而 ρ 决定一个正规基.

我们还将在这里给出正规基定理的另外一种更为成熟的表述，为此引入群 G 的群代数 $\Phi(G)$：$\Phi(G)$ 有基 $G=\{s_1,\cdots,s_n\}$，其乘法由 $(\Sigma\alpha_i s_i)(\Sigma\beta_j s_j)=\Sigma\alpha_i\beta_j s_j s_i=\Sigma\alpha_i\beta_j s_{i_j}$ 确定(参看卷 1 的中译本 p.89 习题 39 的第 2 题)。现对 $\Phi(G)$ 考虑两个右模：第一个是按常规考虑的 $\Phi(G)$ 本身，$xa(x\in\Phi(G),\ a\in\Phi(G))$ 是代数积；第二个是将 P 看成由 $\rho a=\Sigma\alpha_i\rho^{s_i}$ (这里 $a=\Sigma\alpha_i s_i$ 是 $\Phi(G)$ 中的元) 定义的 $\Phi(G)$ 模. 显然对于这个乘法模的公理全被满足，而正规基定理恰好就是这两个模同构这个命题. 事实上，令 (ρ^{s_i}) 是一个正规基并考虑由 Φ 上的 $\Phi(G)$ 到 Φ 上的 P 内的将 s_i 映成 ρ^{s_i} 的线性映射，这是一个 Φ 线性同构，而且如果 $x=\Sigma\xi_i s_i$，则 $xs_j=\Sigma\xi_i s_{i_j}\to\sum_i\xi_i\rho^{s_{i_j}}=\sum_i\xi_i\rho^{s_j s_i}=(\Sigma\xi_i\rho^{s_i})^{s_j}$. 因此，若我们用 x' 表示 x 的象，则 $x's_j=(xs_j)'$. 由此推得 $x'a=(xa)'$ 对一切 $a\in\Phi(G)$ 成立，故我们有一个 $\Phi(G)$ 同构. 反之，容易检

验：若 $x \to x'$ 是 $\Phi(G)$ 到 P 上的一个 $\Phi(G)$ 同构，则 $(s_1 = 1, s_2, \cdots, s_n)$ 的象是 P/Φ 的一个正规基.

习　题　13

1. 证明定理 16 的如下推广：设 $f(x_1^{(1)}, \cdots, x_m^{(1)}, x_1^{(2)}, \cdots, x_m^{(2)}, \cdots, x_1^{(r)}, \cdots, x_m^{(r)})$ 是含未定元 $x_i^{(j)}$ 的一个非零多项式，则存在 $\eta_1, \cdots, \eta_r \in E$ 使 $f(\eta_1^{s_1}, \cdots, \eta_1^{s_m}, \cdots, \eta_r^{s_1}, \cdots, \eta_r^{s_m}) \neq 0$.

13. 有限域　有限域的主要结果将作为伽罗瓦理论的应用得出，现在我们就来推导这些结果，同时还将建立有限基域的本原元及正规基的定理.

我们首先要指出的是：任一有限域 P 都是特征 $p \neq 0$ 的（因为否则 P 会包含一个与有理数域同构的子域），因此 P 的素域 Φ_0 必同构于 $I_p = I/(p)$. 若 Φ 是任一子域，则当然有 $[P:\Phi] = n < \infty$. 若 $(\rho_1, \cdots, \rho_n)$ 是 P 在 Φ 上的一个基，每个元 $\rho \in P$ 只能用唯一的一种方法写成 $\sum_1^n \alpha_i \rho_i (\alpha_i \in \Phi)$. 若基数 $|\Phi| = q$，则由此显然有 $|P| = q^n$. 特别地，若 $[P:\Phi_0] = N$，Φ_0 为素域，则 $|P| = p^N$. 这表明任一有限域的元的个数是它的特征的一个方幂.

其次我们证明：对于任一素数的方幂 p^N，必存在一个有 p^N 个元的域，而且在同构意义下，这个域是唯一的. 我们先证唯一性：设 P 是一个域，其基数 $|P| = p^N$，显然 P 的素域 Φ_0 与 I_p 同构. 若 ρ 是 P 的一个非零元，则 $\rho^{p^N-1} = 1$，这是因为 P 的非零元的乘群 P^* 的阶等于 $p^N - 1$；我们还有 $\rho^{p^N} = \rho$，这个等式对于每个 $\rho \in P$ 都成立. 因此 P 的每个元都是 $x^{p^N} - x = 0$ 的一个根，而且 $x^{p^N} - x \in \Phi_0[x]$，这里 Φ_0 是素域，故有

$$(13) \qquad x^{p^N} - x = \prod_1^{p^N} (x - \rho_i),$$

这里 ρ_i 是 P 的元. 这表明 P/Φ_0 是多项式 $x^{p^N} - x$ 的一个分裂域. 现设 P′ 是基数 $|P'| = p^N$ 的另一域，则 P′ 有特征 p，故它的

素域 $\Phi_0'\cong\Phi_0$. 又 P'/Φ_0 是 $x^{p^N}-x$ 的一个分裂域，故由分裂域的唯一性定理知 $\mathrm{P}'\cong\mathrm{P}$.

刚才使用的方法也可证明基数为 $|\mathrm{P}|=p^N$ (p 为一素数)的域 P 的存在性. 为此我们由有 p 个元的 $\Phi_0=I_p$ 开始,然后令 P 为 $x^{p^N}-x$ 在 Φ_0 上的一个分裂域，Σ 为 $x^{p^N}-x=0$ 的包含于 P 中的根的集. 由于导数 $(x^{p^N}-x)'=-1$, $x^{p^N}-x=0$ 有不同的根,故 $|\Sigma|=p^N$. 其次我们要注意 Σ 是一个子域,这是因为: 如果 $\xi,\eta\in\Sigma$, 则 $\xi^{p^N}=\xi$, $\eta^{p^N}=\eta$, 故

$$(\xi-\eta)^{p^N}=\xi^{p^N}-\eta^{p^N}=\xi-\eta,\ (\xi\eta)^{p^N}=\xi^{p^N}\eta^{p^N}=\xi\eta,$$

而且当 $\eta\neq 0$ 时, $(\eta^{-1})^{p^N}=(\eta^{p^N})^{-1}=\eta^{-1}$, 故有 $\Sigma\supseteq\Phi_0$. 因为 P 是 $x^{p^N}-x$ 的一个分裂域, $\mathrm{P}=\Phi_0(\Sigma)=\Sigma$. 从而有 $|\mathrm{P}|=|\Sigma|=p^N$.

下面证明关于本原元的定理: 若 Φ 是一个有限域而且 P 是 Φ 的一个有限维扩张，则 $\mathrm{P}=\Phi(\theta)$. 显然在此条件下 P 是有限域，现在我们来证明其乘法群 P^* 是循环群. 这是下述一般结果的推论:

引理 1. 一个域的乘法群的任一有限子群 A 都是循环群.

证 设 m 是 A 的阶,而 m' 是 A 的元的最高阶,我们知道,如果 a,b 是一个有限交换群的两个元,则在此群中存在一个元 c, 它的阶是 a 及 b 的阶的最小公倍数(卷 2 的中译本 p.61 习题1). 由此可推得,若 m' 是最高的阶，则对于每个 b 都有 $b^{m'}=1$. 另一方面,方程 $x^{m'}-1=0$ 在一个域中最多只有 m' 个根. 由于 $m'|m$, 我们有 $m'=m$. 还有,若 a 是一个阶为 m 的元,则由 a 生成的循环群 $[a]$ 的阶为 m,故 $A=[a]$.

现设 P 是一个有限域而 Φ 是一个子域,如果选 θ 为循环群 P^* 的一个生成元,则必有 $\mathrm{P}=\Phi(\theta)$.

其次我们考虑有限域的自同构.若特征为 p,则映射 $\pi:\xi\to\xi^p$ 是 P 到 P 内的一个同构. 由于 P 是有限的,因此这是一个自同构. 若 $|\mathrm{P}|=p^N$, 则对每个 $\rho\in\mathrm{P}$ 都有 $\rho^{p^N}=\rho$. 显然 π^i 是自同构 $\xi\to\xi^{p^i}$, 所以有 $\pi^N=1$. 另一方面,若 θ 是群 P^* 的一个生成元，

则当 $m < N$ 时 $\theta^{p^m} \neq \theta$，因此 $\pi^m \neq 1$，从而循环群 $G = [\pi]$ 的阶为 N. 设 Φ 是P的 G 不变元的集，则 Φ 是一个子域且 $[P:\Phi] = N$. 另一方面，我们知道，如果 Φ_0 是素域，则 $[P:\Phi_0] = N$[1]. 因此 $\Phi = \Phi_0$. 我们现在看到域P是它的素域 Φ_0 上的伽罗瓦扩张，而且伽罗瓦群是 $G = [\pi]$. 伽罗瓦对应在P的子域集与 G 的子群集之间给出了一个对应. 由于 G 是 N 阶循环群，对于 N 的每个因子 n 都存在一个且仅存在一个指数为 n 的子群 H. 我们有 $H = \{\tau\}$，这里的 $\tau = \pi^n$. 相对应的有，H 不变元(或 τ 不变元)的对应域 Φ 在 Φ_0 上的维数为 n，因此 $|\Phi| = p^n$. 我们已经证明P的子域 Φ 的阶为 p^n（这里 $n|N$），而且对于每个这样的阶恰有P的一个子域存在，它的阶是所指定的数. 如前所述，P在 Φ 上的伽罗瓦群是循环群 $H = \{\tau\}$. 一般地，我们将称一扩张 P/Φ 为**循环的**、**阿贝尔的**或**可解的**，如果 P/Φ 是有限维伽罗瓦扩张而且它的伽罗瓦群分别是循环的、交换的或可解的. 因此我们可以说，任一有限域都是它的任一子域的一个循环扩张. 从而由以下引理可得对于有限基域的正规基定理:

引理 2. 任一循环扩张 P/Φ 都有一组 Φ 上的正规基.

证　设 s 是 P/Φ 的伽罗瓦群 G 的一个生成元，将 s 看成P在 Φ 上的一个线性变换且设 $\mu(x) \in \Phi[x]$ 是它的最小多项式，则由戴得金无关定理可推出：当 $(G:1) = n$ 时，自同构 $1, s, \cdots, s^{n-1}$ 是P无关的，因此它们还是 Φ 无关的且 $\deg\mu(x) \geq n$. 另一方面，因为 $[P:\Phi] = n$，$\mu(x)$ 的次数不能大于 n（参看卷2的中译本 p.61），故 $\deg\mu(x) = n$. 由于 $s^n = 1$，所以 $\mu(x) = x^n - 1$. 我们知道，存在一个 $\rho \in P$，它关于线性变换 s 的指导多项式是它的最小多项式(见卷2的中译本 p.59). 故 $\rho, \rho^s, \cdots, \rho^{s^{n-1}}$ 是 Φ 无关的，这些元素作成 P/Φ 的一个正规基.

习　题　14

注意：关于有限域的一组习题早已在卷1的中译本 p.105 中给出.

---

1) 原文此处误为 p^N. ——译者注

1. 设 Φ 是一个 $q(=p^N)$ 阶有限域，证明：不可约多项式 $f(x)\in\Phi[x]$ 是 $x^{q^n}-x$ 的一个因子当且仅当 $\deg f(x)|n$. （提示：考虑域 $\Phi[x]/(f(x))$. ）再证：$x^{q^n}-x=\Pi f_i(x)$，这里的 $f_i(x)$ 遍历所有次数是 n 的因子的首项系数为 1 的不可约多项式. 若令 $N(q,r)$ 表示这些次数为 r 的多项式的个数，推导公式

$$N(q,n)=\frac{1}{n}\sum_{r|n}\mu\left(\frac{n}{r}\right)q^r$$

这里的 μ 是牟比乌斯（Möbius）函数（参看卷 1 的中译本 p.112 习题 47 的第 5 题）.

2. 设 $\mathfrak{M}$ 是特征 $p\neq 2$，阶为奇数 q 的有限域 Φ 上的 n 维向量空间，$g(x,y)$ 是 Φ 上的 $\mathfrak{M}$ 的非退化对称双线性型. 证明：若 $n\geq 2$，则在 $\mathfrak{M}$ 中存在一个向量 u 使 $g(u,u)=1$. 应用此结果及卷 2 的中译本 p.135—137 的化简理论证明：$\mathfrak{M}$ 有一个正交基 $(u_1,u_2,\cdots,u_n)$ 使 $g(u_1,u_1)=\delta\neq 0$，而当 $i>1$ 时，$g(u_i,u_i)=1$. 利用此结果证明：元在 Φ 中的任二非奇异对称 $n\times n$ 矩阵是同步的（congredient）当且仅当它们的行列式相差一个在 Φ 中是一个完全平方的乘法因子（$\delta=\delta'\rho^2$）. 证明：恰有两类同步的非奇异对称矩阵.

3. Φ，$\mathfrak{M}$，g 如第 2 题所示. 若 $(e_1,e_2,\cdots,e_n)$ 是一个基，则 $\delta=\det(g(e_i,e_j))$ 称为 g 的一个判别式. 对于 $b\in\Phi$，令 $N(g,b)$ 表示满足 $g(u,u)=b$ 的向量 $u\in\mathfrak{M}$ 的个数，证明

$$N(g,0)=\begin{cases}q^{2\nu-1}-q^{\nu}+q^{\nu-1}, & \text{若 } n=2\nu \text{ 且}(-1)^{\nu}\delta \text{ 不是一个平方数},\\ q^{2\nu-1}+q^{\nu}-q^{\nu-1}, & \text{若 } n=2\nu \text{ 且}(-1)^{\nu}\delta \text{ 是一个平方数},\\ q^{2\nu}, & \text{若 } n=2\nu+1.\end{cases}$$

$$N(g,b)=\begin{cases}q^{2\nu-1}+q^{\nu-1}, & \text{若 } b\neq 0,\ n=2\nu, \text{ 且}(-1)^{\nu}\delta \text{ 不是一个平方数},\\ q^{2\nu-1}-q^{\nu-1}, & \text{若 } b\neq 0,\ n=2\nu, \text{ 且}(-1)^{\nu}\delta \text{ 是一个平方数},\\ q^{2\nu}-q^{\nu}, & \text{若 } b\neq 0,\ n=2\nu+1, \text{ 且}(-1)^{\nu}\delta b \text{ 不是一个平方数},\\ q^{2\nu}+q^{\nu}, & \text{若 } b\neq 0,\ n=2\nu+1, \text{ 且}(-1)^{\nu}\delta b \text{ 是一个平方数}.\end{cases}$$

4. 设 $O(n,g)$ 表示由 g 确定的正交群：$O(n,g)$ 是 M 的使 $g(xA,yA)=g(x,y)$（对所有 $x,y\in M$）的线性变换 A 的群，若 u 是一个非迷向向量，Ou 是 $O(n,g)$ 的使 u 不动的子群，证明 Ou 同构于 $O(n-1,g')$，这里 g' 是 g 在 $(\Phi u)^{\perp}$ 上的限制，应用维特（Witt）定理证明 Ou 在 $O(n,g)$ 中的陪集 OuA 的个数是满足 $g(v,v)=g(u,u)$ 的向量 v 的个数. 应用这个结果及第 3 题建立阶 $(O(n,g):1)$ 的下列公式：

$$(O(n,g):1)=\begin{cases}2\cdot q^{(n-1)^2/4}\prod\limits_{i=1}^{(n-1)/2}(q^{2i}-1), & \text{若 } n \text{ 是奇数},\\ 2\cdot q^{n(n-2)/4}(q^{n/2}-\varepsilon)\prod\limits_{i=1}^{(n-2)/2}(q^{2i}-1), & \text{若 } n \text{ 是偶数},\end{cases}$$

这里当 $(-1)^{\nu}\delta$ 是一个平方数时，$\varepsilon=1$，否则 $\varepsilon=-1$.

14. 正则表示，迹与范数　本节考虑有限维扩域 P/Φ 并定义称为迹与范数的 P 到 Φ 内的映射，这些函数对任意有限维代数都是容易定义的，而且对它们也是很重要的. 因此我们将从考虑 Φ

上的具有基 $(u_1, u_2, \cdots, u_n)$ 的一个有限维代数 $\mathfrak{A}/\Phi$ 开始.我们定义 $\mathfrak{A}/\Phi$ 的一个(有限维)表示为 $\mathfrak{A}/\Phi$ 到一个有限维向量空间 $\mathfrak{M}/\Phi$ 的线性变换代数 $\mathfrak{L}_\Phi(\mathfrak{M})$ 内的一个同态. 若 s 是这样的一个表示: $a \to a^s$, 则定义的条件是:

$$(a+b)^s = a^s + b^s,\ (\alpha a)^s = \alpha a^s, \tag{14}$$
$$(ab)^s = a^s b^s,\ 1^s = 1.$$

这里的 $a, b \in \mathfrak{A}$, $\alpha \in \Phi$, 若 $(x_1, x_2, \cdots, x_N)$ 是 $\mathfrak{M}$ 在 Φ 上的一个基,则我们可以象通常一样确定 a^s 关于这个基的矩阵: 先写

$$x_i a^s = \sum_{j=1}^{N} \alpha_{ij}(a) x_j,\ i = 1, 2, \cdots, N. \tag{15}$$

这给出矩阵 $\alpha(a) = (\alpha_{ij}(a))$ 及 $\mathfrak{A}/\Phi$ 到元在 Φ 中的 $N \times N$ 矩阵代数 Φ_N/Φ 内的映射 $a \to \alpha(a)$. 由于线性变换 A 到它的关于基 $(x_1, x_2, \cdots, x_N)$ 的矩阵 (α) 的映射 $A \to (\alpha)$ 是一个同构. 映射 $a \to \alpha(a)$ 是 $\mathfrak{A}/\Phi$ 到 Φ_N/Φ 内的一个同态, 这个同态称为一个矩阵表示. 我们还记得: 若将基 $(x_1, x_2, \cdots, x_N)$ 换为另一基 $(y_1, y_2, \cdots, y_N)$, 这里 $y_i = \Sigma \mu_{ij} x_j$, 则由 S 及这个基确定的矩阵表示是 $a \to (\mu)\alpha(a)(\mu)^{-1}$, 其中 $(\mu) = (\mu_{ij})$ (参看卷 2 的中译本 p.38).

$\mathfrak{A}/\Phi$ 的最重要的表示是所谓正则表示 R, 这里 $a^R = a_R$. 即由 a 定义的右乘 $x \to xa$. 直接检验可知 a_R 是 $\mathfrak{A}$ 在 Φ 上的一个线性变换,而且 $a \to a_R$ 是一个代数同态 (参看卷 1 的中译本 p.77). 由于 $\mathfrak{A}$ 有一单位元,故 $a \to a_R$ 是 1—1 的,因而是 $\mathfrak{A}/\Phi$ 到 $\mathfrak{L}_\Phi(\mathfrak{A})$ 内的一个同构. 由于 $xa_R = xa$, 我们要想得到对应于 $\mathfrak{A}/\Phi$ 的基 $(u_1, u_2, \cdots, u_n)$ 的矩阵表示, 可先将乘积 $u_i a$ 写作 u_i 的 Φ 线性组合

$$u_i a = \Sigma \rho_{ij}(a) u_j,\ j = 1, 2, \cdots, n. \tag{16}$$

然后记 $\rho(a) = (\rho_{ij}(a))$, 我们就可得到矩阵表示 $a \to \rho(a)$, 它是 1—1 的. 又因 $1_R = 1$, $\rho(1) = 1$, 这里的 1 是单位矩阵, 和通常情况一样,将基变成 $(v_1, v_2, \cdots, v_n)$, 这里 $v_i = \Sigma \mu_{ij} u_j$, 给出新的矩阵表示 $a \to \sigma(a)$, 其中

(17) $$\sigma(a)=(\mu)\rho(a)(\mu)^{-1},\ (\mu)=(\mu_{ij}).$$

作为例子我们看具有单独一个生成元的代数 $\mathfrak{A}=\Phi[a]$：由于 $[\mathfrak{A}:\Phi]<\infty$，$\Phi[a]\cong\Phi[x]/(f(x))$，这里 $f(x)$ 是一个首项系数为 1 的非零多项式．我们有 $f(a)=0$ 且 $f(x)$ 是以 a 为其一根的、次数最低的、非零的首项系数为 1 的多项式，因此多项式 $f(x)$ 是 a 的最小多项式(导言 p.5)而且 $\Phi[a]$ 有基 $(1, a, \cdots, a^{n-1})$，其中 $n=[\mathfrak{A}:\Phi]=\deg f(x)$．假设

(18) $$f(x)=x^n-\alpha_1x^{n-1}+\cdots+(-1)^n\alpha_n,\ \alpha_i\in\Phi,$$

则有关系

(19) $$\begin{aligned}&1a=a,\ aa=a^2,\cdots,\ a^{n-2}a=a^{n-1},\\&a^{n-1}a=\alpha_1a^{n-1}-\alpha_2a^{n-2}+\cdots+(-1)^{n-1}\alpha_n.\end{aligned}$$

这些关系表明：若 $\rho(a)$ 表示 a_R 关于 $(1, a,\cdots, a^{n-1})$ 的矩阵，则我们有

(20) $$\rho(a)=\begin{bmatrix}0 & 1 & 0 & \cdot & \cdot & \cdot\\ 0 & 0 & 1 & \cdot & \cdot & \cdot\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ (-1)^{n-1}\alpha_n & \cdot & \cdot & \cdot & -\alpha_2 & \alpha_1\end{bmatrix}$$

它称为多项式 $f(x)$ 的**友矩阵**，从理论上来说，只要我们知道了这个矩阵，就能对 $\Phi[a]$ 中的任意元 b 求出 $\rho(b)$，因为 b 是 a 的多项式．

我们再考虑一般情况并定义元 $a\in\mathfrak{A}$ 的**特征多项式**为 $\mathfrak{A}$ 中线性变换 a_R (或其对应矩阵 $\rho(a)$) 的特征多项式

(21) $$f_a(x)=\det(x1-\rho(a)).$$

由(17)有

$$x1-\sigma(a)=(\mu)(x1-\rho(a))(\mu)^{-1},$$

它表示

$$\begin{aligned}\det(x1-\sigma(a))&=\det(\mu)(x1-\rho(a))(\mu)^{-1}\\&=\det(\mu)\det(x1-\rho(a))\det(\mu)^{-1}\\&=\det(x1-\rho(a)).\end{aligned}$$

可见 $f_a(x)$是与 $\mathfrak{A}/\Phi$的基的选择无关的，我们可将特征多项式写为

(22) $f_a(x)=x^n-T(a)x^{n-1}+\cdots+(-1)^nN(a)$.

我们有 $T(a)=\mathrm{trace}\rho(a)=\sum_1^n\rho_{ii}(a)$, $N(a)=\det(\rho(a))$. 并分别称它们为 Φ 上的 $\mathfrak{A}$ 中 a 的迹与范数. 有时需要区别代数的基域及该代数本身,此时将用 $T_{\mathfrak{A}|\Phi}(a)$ 表示 $T(a)$, 用 $N_{\mathfrak{A}|\Phi}(a)$ 表示 $N(a)$. 由于迹是矩阵的线性函数以及 $a\to\rho(a)$ 是线性的,显然 $a\to T_{\mathfrak{A}|\Phi}(a)$ 是 $\mathfrak{A}$ 到 Φ 内的一个线性映射.又因 $\rho(1)=1$, 我们有 $T_{\mathfrak{A}|\Phi}(1)=n1$ 及 $T_{\mathfrak{A}|\Phi}(\alpha a)=\alpha T_{\mathfrak{A}|\Phi}(a)$. 因此我们有下列关系:

$$
\begin{aligned}
&T_{\mathfrak{A}|\Phi}(a+b)=T_{\mathfrak{A}|\Phi}(a)+T_{\mathfrak{A}|\Phi}(b),\\
(23)\qquad &T_{\mathfrak{A}|\Phi}(\alpha a)=\alpha T_{\mathfrak{A}|\Phi}(a),\ \alpha\in\Phi,\\
&T(1)=n1.
\end{aligned}
$$

由于 $a\to\rho(a)$ 是可乘的, $A\to\det A$ 是矩阵集的一个可乘映射, 因此我们有 $N_{\mathfrak{A}|\Phi}(ab)=N_{\mathfrak{A}|\Phi}(a)N_{\mathfrak{A}|\Phi}(b)$. 显然还有 $N_{\mathfrak{A}|\Phi}(\alpha a)=\alpha^nN_{\mathfrak{A}|\Phi}(a)$ 及 $N_{\mathfrak{A}|\Phi}(1)=1$. 因此我们有

$$
\begin{aligned}
&N_{\mathfrak{A}|\Phi}(ab)=N_{\mathfrak{A}|\Phi}(a)N_{\mathfrak{A}|\Phi}(b),\\
(24)\qquad &N_{\mathfrak{A}|\Phi}(\alpha a)=\alpha^nN_{\mathfrak{A}|\Phi}(a),\ \alpha\in\Phi,\\
&N(1)=1.
\end{aligned}
$$

我们还知道,根据哈密顿-凯利定理, $\rho(a)$ 是 $f_a(x)=0$ 的一个根,若运用同构 $\rho(b)\to b$, 就可见 $f_a(a)=0$. 因此有

(25) $a^n-T(a)a^{n-1}+\cdots+(-1)^nN(a)1=0$.

设 $m_a(x)$ 是 $\rho(a)$ (或 a_R) 的最小多项式,由于 $b\to\rho(b)$ 是一个同构,显然 $m_a(x)$ 是 a 的最小多项式. 我们还知道, 矩阵的最小多项式是它的特征多项式是一个因子且两者 $\Phi[x]$ 中有相同的不可约因子, 所不同的只是因子的重数 (卷 2 的中译本 p.88 或 p.90)

迹函数可用来定义代数 $\mathfrak{A}/\Phi$ 上的一个重要双线性型, 这就是正则迹型

(26) $(a,b)=T_{\mathfrak{A}|\Phi}(ab)$.

显然这个在 Φ 中取值的函数服从以下法则:

$$(27)\quad \begin{aligned}&(a, b_1+b_2)=(a, b_1)+(a, b_2),\\&(a_1+a_2, b)=(a_1, b)+(a_2, b),\\&\alpha(a, b)=(\alpha a, b)=(a, \alpha b),\\&(ab, c)=(a, bc)\ (=T_{\mathfrak{A}|\Phi}(abc)).\end{aligned}$$

我们还知道，如果 M，N 都是矩阵，则 $\mathrm{tr}MN=\mathrm{tr}NM$（卷 2 的中译本 p.92）。由此可得

$$(28)\qquad (a, b)=(b, a),$$

因此 (a, b) 是一个对称双线性型。我们定义 Φ 上的 $\mathfrak{A}$ 关于基 $(u_1, u_2, \cdots, u_n)$ 的**判别式**为

$$(29)\qquad \delta(u_i)=\det((u_i, u_j))=\det(T_{\mathfrak{A}|\Phi}(u_iu_j)).$$

易见：若将 $(u_1, \cdots, u_n)$ 用基 $(v_1, \cdots, v_n)$（这里 $v_i=\Sigma\mu_{ij}u_j$）代替，则矩阵 $((u_i, u_j))$ 变成 $(v_i, v_j)=M((u_i, u_j))M'$，$M=(\mu_{ij})$（卷 2 的中译本 p.132），因此关于 (v_i) 的判别式是 $\delta(u_i)\mu^2$，$\mu=\det M$。

现设 E 是 Φ 的一个子域，它在 Φ 中有有限余维数，则 $\mathfrak{A}\supseteq\Phi\supseteq E$，而且 $[\mathfrak{A}:E]=[\mathfrak{A}:\Phi][\Phi:E]$ 是有限数，故若将 $\mathfrak{A}$ 看作 E 上的一个向量空间，则它是有限维的，因此 $\mathfrak{A}$ 是 E 上的有限维代数。我们就可以对代数 $\mathfrak{A}/E$ 进行上述的全部考虑。也可将 Φ 作为 E 上的一个代数考虑并定义 $T_{\mathfrak{A}|E}$，$T_{\Phi|E}$，$N_{\mathfrak{A}|E}$，$N_{\Phi|E}$ 以及 $T_{\mathfrak{A}|\Phi}$，$N_{\mathfrak{A}|\Phi}$。我们现在来建立联系这些函数的基本传递性关系。

若 $\Phi\supseteq E$，则

$$(30)\qquad T_{\mathfrak{A}|E}(a)=T_{\Phi|E}(T_{\mathfrak{A}|\Phi}(a)).$$

$$(31)\qquad N_{\mathfrak{A}|E}(a)=N_{\Phi|E}(N_{\mathfrak{A}|\Phi}(a)).$$

如前仍设 $(u_1, \cdots, u_n)$ 是 $\mathfrak{A}/\Phi$ 的一个基，而 $(\gamma_1, \gamma_2\cdots, \gamma_h)$ 是 Φ/E 的一个基，则

$$(32)\qquad (\gamma_1u_1, \gamma_2u_1, \cdots, \gamma_hu_1; \gamma_1u_2, \cdots, \gamma_hu_2; \cdots, \gamma_hu_n)$$

是 $\mathfrak{A}/E$ 的一个基；设 $\rho\in\Phi$，我们可将它写成

$$(33)\qquad \gamma_q\rho=\Sigma\lambda_{qt}(\rho)\gamma_t,\quad q, t=1, \cdots, h$$

故有同构 $\rho\to(\lambda(\rho))$，这里的 $\lambda(\rho)$ 是元在 E 中的矩阵 $(\lambda_{qt}(\rho))$，故 $T_{\Phi|E}(\rho)=\Sigma\lambda_{qq}(\rho)$ 及 $N_{\Phi|E}(\rho)=\det(\lambda(\rho))$。将

(16)代入(33)得

$$(34)\quad (\gamma_q u_i)a = \Sigma\gamma_q\rho_{ij}(a)u_j = \Sigma\lambda_{qt}(\rho_{ij}(a))\gamma_t u_j,\ i,j=1,\cdots,n;\quad q,t=1,\cdots,h.$$

这表明若基 $(\gamma_q u_i)$ 按(32)排定次序,则 a_R 在 $\mathfrak{A}/E$ 中的矩阵是

$$(35)\qquad \Lambda(a) = \begin{bmatrix} \lambda(\rho_{11}) & \lambda(\rho_{12})\cdots\lambda(\rho_{1n}) \\ \lambda(\rho_{21}) & \lambda(\rho_{22})\cdots\lambda(\rho_{2n}) \\ \cdot & \cdot\ \cdots\ \cdot \\ \lambda(\rho_{n1}) & \lambda(\rho_{n2})\cdots\lambda(\rho_{nn}) \end{bmatrix}$$

这里 $\lambda(\rho_{ij})$ 是一个元在 E 中的 $h\times h$ 矩阵,而 ρ_{ij} 则是 $\rho_{ij}(a)$ 的简写. 由(35)易见:

$$\begin{aligned} T_{\mathfrak{A}|E}(a) &= \mathrm{tr}\Lambda(a)\ (\text{这里 tr} \equiv \text{迹}) \\ &= \mathrm{tr}\lambda(\rho_{11}) + \mathrm{tr}\lambda(\rho_{22}) + \cdots + \mathrm{tr}\lambda(\rho_{nn}) \\ &= \mathrm{tr}\lambda(\rho_{11}+\rho_{22}+\cdots+\rho_{nn}) \\ &= \mathrm{tr}\lambda(T_{\mathfrak{A}|\Phi}(a)) \\ &= T_{\Phi|E}(T_{\mathfrak{A}|\Phi}(a)). \end{aligned}$$

这就是公式(30)

要证明公式(31)需要用到下面推导的行列式的一个一般传递性质(卷2,中译本 p.120 习题的第2题): 设有一个元在域 E 中的 $nh\times nh$ 矩阵,我们将它分割成一个 $n\times n$ 矩阵 $\Lambda=(\lambda_{ij})$, 其中每个 λ_{ij} 是一个 $h\times h$ 矩阵, 而且 λ_{ij} 全部交换、这等价于假设 λ_{ij} 全部属于矩阵代数 Φ_h 的一个交换子代数 $\mathfrak{B}$, 这恰是(35)的矩阵 $\Lambda(a)$ 与子块 $\lambda(\rho_{ij})$ 所处的情况. 由于 $\lambda_{ij}\in\mathfrak{B}$ 及 $\mathfrak{B}$ 是交换的,所以行列式的通常定义及性质仍有效,我们可考虑

$$(36)\qquad \det{}_n(\Lambda) = \sum_P \varepsilon_P\lambda_{1i_1}\lambda_{2i_2}\cdots\lambda_{ni_n},$$

这里是对 $(1,2,\cdots,n)$ 的所有置换 $(i_1i_2\cdots i_n)$ 求和的, 而 $\varepsilon_P=1,-1$ 则视 P 为偶置换或奇置换而定. 上面所规定的$\det_n(\Lambda)$是 Φ_h 的一个元,所以我们能取它的通常行列式, 我们来建立下列公式:

$$(37)\qquad \det(\det{}_n(\Lambda)) = \det\Lambda,$$

这里 $\det\Lambda$ 是 $nh\times nh$ 矩阵的通常行列式.

要证明这个结果，我们可将基域 E 扩张到所有矩阵 λ_{ij} 的特征多项式的积在 E 上的一个分裂域，若能在这个域中证明这个结果就足够了. 不失一般性，我们可以假定 E 包含所有 λ_{ij} 的特征根，交换线性变换集理论(卷 2 的中译本 p. p.118—119)表明存在一矩阵 $\mu\varepsilon E_h$ 使每个 $\mu^{-1}\lambda_{ij}\mu$ 是三角形矩阵:

$$(38)\qquad \mu^{-1}\lambda_{ij}\mu=\eta_{ij}=\begin{bmatrix}\rho_{ij_1} & & & * \\ & \rho_{ij_2} & & \\ & & \ddots & \\ 0 & & & \rho_{ij_h}\end{bmatrix}.$$

因此，若设

$$(39)\qquad M=\begin{bmatrix}\mu & & & \\ & \mu & & \\ & & \ddots & \\ & & & \mu\end{bmatrix},$$

则

$$(40)\qquad M^{-1}AM=\begin{bmatrix}\eta_{11} & \eta_{12} & \cdots & \eta_{1n} \\ \eta_{21} & \eta_{22} & \cdots & \eta_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ \eta_{n1} & \eta_{n2} & \cdots & \eta_{nn}\end{bmatrix}.$$

我们有 $\det A=\det M^{-1}AM$，由于 $\eta_{ij}=\mu^{-1}\lambda_{ij}\mu$,

$$\det{}_n M^{-1}AM=\mu^{-1}(\det{}_n A)\mu.$$

因此 $\det(\det_n M^{-1}AM)=\det(\det_n A)$，故只须检验下式即可:

$$(41)\qquad \det(\det{}_n M^{-1}AM)=\det M^{-1}AM.$$

直接由 $\det_n$ 的定义及三角形矩阵的相乘、相加方法可得

$$(42)\qquad \det{}_n M^{-1}AM=\begin{bmatrix}\det\rho_1 & & & * \\ & \det\rho_2 & & \\ & & \ddots & \\ 0 & & & \det\rho_h\end{bmatrix},$$

其中

$$(43)\qquad \rho_k=\begin{bmatrix}\rho_{11k} & \rho_{12k} & \cdots & \rho_{1nk} \\ \rho_{21k} & \rho_{22k} & \cdots & \rho_{2nk} \\ \cdot & \cdot & \cdots & \cdot \\ \rho_{n1k} & \rho_{n2k} & \cdots & \rho_{nnk}\end{bmatrix}.$$

因此

$$(44) \qquad \det(\det_n M^{-1}AM) = \det\rho_1 \det\rho_2 \cdots \det\rho_h.$$

其次我们还需要计算 $\det M^{-1}AM$. 为此我们作下列的行与列的置换：对于 $i=1,2,\cdots,n$ 及 $j=1,2,\cdots,h$，使

列 $(i-1)h+j \to$ 列$(j-1)n+i$,

行 $(i-1)h+j \to$ 行$(j-1)n+i$.

这样就给出矩阵

$$(45) \qquad \begin{bmatrix} \rho_1 & & & * \\ & \rho_2 & & \\ & & \ddots & \\ & & & \rho_h \end{bmatrix},$$

其中 ρ_k 如公式(43)所示. 因此由拉普拉斯 (Laplace) 展开式，$\det M^{-1}AM = \det\rho_1\det\rho_2\cdots\det\rho_h = \det(\det_n M^{-1}AM)$. 这就证明了所需要的公式(37).

现将这个结果应用于范数，我们有 $N_{\mathfrak{A}|\Phi}(a) = \det(\rho_{ij}(a)) \in \Phi$ 及

$$N_{E|\Phi}N_{\mathfrak{A}|\Phi}(a) = \det(\lambda(\det\rho_{ij})).$$

由于 $\rho \to \lambda(\rho)$ 是一个同构，我们有

$$(\lambda(\det\rho_{ij})) = \det_n(\lambda(\rho_{ij}))$$

因此由公式(37)

$$\det\lambda(\det\rho_{ij}) = \det\det_n(\lambda(\rho_{ij})) = \det A(a).$$

由 $\det A(a) = N_{\mathfrak{A}|E}(a)$，我们得到范数公式(31). 我们现在将所有这些限制在 $\mathfrak{A}$ 是一个域 P 的情况[1]. 我们知道任意 $a \in P$ 的最小多项式 $m_a(x)$ 都是不可约的，因此特征多项式 $f_a(x) = m_a(x)^r$. 我们有 $[P:\Phi] = n = \deg f_a(x)$，$[\Phi(a):\Phi] = \deg m_a(x)$，因此 $r = \deg f_a(x)/\deg m_a(x) = [P:\Phi]/[\Phi(a):\Phi] = [P:\Phi(a)]$. 故有

$$(46) \qquad f_a(x) = m_a(x)^{[P:\Phi(a)]}$$

我们还要推导几个关于一个域的范数与迹的重要公式，让我

---

1) 在此情况下证明范数传递性公式的一个简易方法将在下面习题的第二题中指出. ——著者注.

们先看可分域的情况：设 P/Φ 为有限维可分扩张，Ω/Φ 是 P/Φ 的正规闭包，则 Ω/Φ 是伽罗瓦扩张，而且对于 Ω/Φ 的伽罗瓦群 G 有 $[\Omega:\Phi]=[G:1]$. 设 H 是 G 的对应于 P/Φ 的子群(即 Ω/P 的伽罗瓦群). 由于 $[\mathrm{P}:\Phi]=n$, 指数 $(G:H)=n$, 我们有 n 个不同的陪集 $Hs'_1, Hs'_2, \cdots, Hs'_n$. 若 s_i 表示 s'_i 在 P 上的限制，则 $s_1, s_2, \cdots, s_n$ 是 P/Φ 到 Ω/Φ 内的不同的同构，而且它们是 P/Φ 到 Ω/Φ 内的全部同构(§7). 次设 $\rho\in\mathrm{P}$ 且 K 是 G 的对应于 $\Phi(\rho)$ 的子群，则 $G\supseteq K\supseteq H$. 设 $t'_1, \cdots, t'_m$ 是 G 中陪集 Kt' 的一个完全代表系，$u'_1, \cdots, u'_r$ 是 K 中陪集 Hu' 的一个完全代表系，则我们有 $G=\bigcup Kt'_j$, $K=\bigcup Hu'_k$. 故 $G=\bigcup Hu'_kt'_j$, 这 mr 个元 $u'_kt'_j$ 作成 G 中 H 的陪集的一个完全代表系，我们可以假设这些元就是我们前面讲的 s'_i. 这些 t'_j 在 $\Phi(\rho)$ 上的限制给出 $\Phi(\rho)/\Phi$ 到 Ω/Φ 内的所有同构，而且它们是互异的；由于 ρ 生成 $\Phi(\rho)$, 故可推知元 $\rho^{t'_1}, \rho^{t'_2}, \cdots, \rho^{t'_m}$ 是互异的，而且它们包含所有的共轭元 $\rho^{s'}$, 这里 $s\in G$. 因此 ρ 在 Φ 上的最小多项式是

$$m_\rho(x)=\prod_{j=1}^{m}(x-\rho^{t'_j}).$$

但是我们还有 $\rho^{u'_kt'_j}=\rho^{t'_j}$ 对一切 k 及 j 成立，因此

$$\prod_{i=1}^{n}(x-\rho^{s'_i})=\prod_{k=1}^{r}\prod_{j=1}^{m}(x-\rho^{u'_kt'_j})=m_\rho(x)^r.$$

另一方面，$r=[\mathrm{P}:\Phi(\rho)]$, 故若在(46)中使 $a=\rho$ 就可知特征多项式

$$f_\rho(x)=\prod_{1}^{n}(x-\rho^{s_i}), \tag{47}$$

这里 $s_1, s_2, \cdots, s_n$ 是 P/Φ 到它的正规闭包 Ω/Φ 内的不同的同构，将这公式与(22)对比就可得到在可分情况下的迹与范数公式：

$$T_{\mathrm{P}/\Phi}(\rho)=\sum_{1}^{n}\rho^{s_i},\quad N_{\mathrm{P}/\Phi}(\rho)=\prod_{1}^{n}\rho^{s_i}. \tag{48}$$

其次考虑 P/Φ 是纯不可分的、特征 $p\neq 0$ 的域的情况. 此时有 $[\mathrm{P}:\Phi]=p^f$. 设 $\rho\in\mathrm{P}$, 其最小多项式 $m_\rho(x)$ 有形式

$x^{p^e}-\alpha=(x-\rho)^{p^e}$，由于 $P/\Phi(\rho)$ 是纯不可分的，$[P:\Phi(\rho)]=p^g$，$p^f=[P:\Phi]=[P:\Phi(\rho)]\cdot[\Phi(\rho):\Phi]=p^g p^e$，因此 $f=g+e$。由(46)，特征多项式是

(49) $$f_\rho(x)=(x^{p^e}-\alpha)^{p^g}=(x-\rho)^{p^f}.$$

这就证明了

(50) $$T_{P|\Phi}(\rho)=[P:\Phi]\rho,\ N_{P|\Phi}(\rho)=\rho^{[P:\Phi]}.$$

现设 P/Φ 是任意域，Σ/Φ 是极大可分子域，Ω/Φ 是 P/Φ 的正规闭包，则 Ω/Φ 包含 Σ/Φ 的正规闭包 Δ/Φ。我们仍假设其特征 $p\neq 0$，则 $[P:\Sigma]=p^f$，$f\geqslant 0$，这就是不可分次数 $[P:\Phi]_i$ (§10)。若 $\rho\in P$，由(50)及(47)有

$$\begin{aligned}N_{P|\Phi}(\rho)&=N_{\Sigma|\Phi}(N_{P|\Sigma}(\rho))=N_{\Sigma|\Phi}(\rho^{[P:\Phi]_i})\\&=(\rho^{[P:\Phi]_i})^{s_1}(\rho^{[P:\Phi]_i})^{s_2}\cdots(\rho^{[P:\Phi]_i})^{s_n}\end{aligned}$$

这里的 $s_1,s_2,\cdots,s_n$ 是 Σ/Φ 到 Δ/Φ 内的不同的同构，易见每个 s_i 是 P/Φ 到 Ω/Φ 内的一个同构的限制，而且 P/Φ 到 Ω/Φ 内的相异同构在 Σ/Φ 上有相异的限制，并将这个域映入 Δ/Φ（见§10习题的第一题）。上述公式还可改写为

(51) $$N_{P|\Phi}(\rho)=(\rho^{s_1}\rho^{s_2}\cdots\rho^{s_n})^{[P:\Phi]_i}$$

这里 $s_1,s_2,\cdots,s_n$ 可看作 P/Φ 到 Ω/Φ 内的不同的同构。用完全相同的方法可得：

(52) $$T_{P|\Phi}(\rho)=[P:\Phi]_i(\rho^{s_1}+\rho^{s_2}+\cdots+\rho^{s_n}).$$

若 P 不是 Φ 上的可分域，则 $f>0$ 而且 $[P:\Phi]_i=p^f$ 能被 p 整除，因此对于不可分的 P/Φ 来说，$T_{P|\Phi}(\rho)\equiv 0$。

下面我们还要得到 P/Φ 关于一个基 $(\rho_1,\rho_2,\cdots,\rho_n)$ 的判别式的一些公式，它就是

(53) $$\delta=\det(T_{P|\Phi}(\rho_i\rho_j)).$$

若 P/Φ 是不可分的，因 $T_{P|\Phi}=0$，故 $\delta=0$。现设 P/Φ 是可分的，如前仍设 $s_1,s_2,\cdots,s_n$ 是 P/Φ 到 Ω/Φ 内的同构，今考虑矩阵

(54) $$A=(\rho_i^{s_j})(i,j=1,2,\cdots,n).$$

我们在定理 16 的证明中已经看到 $\det A\neq 0$，我们来考察矩阵

AA'（这里 A' 是矩阵 A 的转置矩阵），它的 (i, j) 元是

$$\rho_i^{\prime 1}\rho_j^{\prime 1} + \rho_i^{\prime 2}\rho_j^{\prime 2} + \cdots + \rho_i^{\prime n}\rho_j^{\prime n} = T_{P|\Phi}(\rho_i\rho_j). \tag{55}$$

因此 $\delta = \det AA'$，故有

$$\delta = (\det A)^2, A = (\rho_i^{\prime j}). \tag{56}$$

由于 $\det A \neq 0$，这式表示 $\delta \neq 0$. 我们还知道由这个结果可推出迹双线性型 $(\rho, \sigma) = T_{P|\Phi}(\rho\sigma)$ 是非退化的（卷 2 的中译本 p.124），因此我们有下列

定理 18 若 P/Φ 是有限维可分的，则其迹型（trace form）$(\rho, \sigma) = T_{P|\Phi}(\rho\sigma)$ 是非退化的且 P/Φ 的判别式 $\delta \neq 0$.

设 θ 是有限维可分扩张的一个本原元，则由(46)易知 θ 的特征多项式 $f(x)$ 与它的最小多项式相同. 在 $\Omega[x]$ 中我们有 $f(x) = (x - \theta_1)(x - \theta_2)\cdots(x - \theta_n)$，$\theta_1 = \theta$，且各 θ_i 是相异的. 若 $f'(x)$ 是 $f(x)$ 的导数，则

$$f'(\theta) = (\theta - \theta_2)(\theta - \theta_3)\cdots(\theta - \theta_n), \tag{57}$$

因为 $f'(x) \in \Phi[x]$，所以这个元包含于 $P = \Phi(\theta)$ 之中. 元 $f'(\theta)$ 称为 θ 的**差异**. 我们将证明由基 $(1, \theta, \theta^2, \cdots, \theta^{n-1})$ 确定的判别式 δ 是

$$\delta = (-1)^{\frac{n(n-1)}{2}} N_{P|\Phi}(f'(\theta)). \tag{58}$$

我们有 $\delta = \det T_{P|\Phi}(\theta^{i-1}\theta^{j-1})$. 显然我们有一个将 θ 映入 θ_i 的 $(1 \leqslant i \leqslant n)\Phi(\theta)/\Phi$ 到 Ω/Φ 内的同构，因此 θ_i 是 θ 的共轭元 $\theta^{\prime i}$ 且 $(\theta^k)^{\prime i} = \theta_i^k$. (54) 的对于基 $(1, \theta, \theta^2, \cdots, \theta^{n-1})$ 的矩阵 A 现在变为

$$A = \begin{bmatrix} 1 & 1 & \cdots 1 \\ \theta_1 & \theta_2 & \cdots \theta_n \\ \cdot & \cdot & \cdots \cdot \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots \theta_n^{n-1} \end{bmatrix}.$$

$\det A$ 是著名的范得蒙得（Vandermonde）行列式，它的值是

$\prod_{j>i} (\theta_j - \theta_i)$，因此(56)给出判别式公式

$$(59)\qquad \delta=\prod_{i<j}(\theta_i-\theta_j)^2,\ i,j=1,2,\cdots,n.$$

另一方面，$f'(\theta)=\prod_{i\neq 1}(\theta_1-\theta_i)$，利用 s_j，将 θ_1 映入 θ_j 可得

$f'(\theta)^{s_j}=\prod_{i\neq j}(\theta_j-\theta_i)$，于是

$$(60)\qquad N_{P|\Phi}(f'(\theta))=(-1)^{\frac{n(n-1)}{2}}\prod_{i<j}(\theta_i-\theta_j)^2.$$

比较(59)和(60)，就证明了(58)。

习　题　15

1. 设 $\mathfrak{A}$ 是代数 $\Phi[x]/(x^n-1)$，则 $\mathfrak{A}$ 有基 $(1,\theta,\cdots,\theta^{n-1})$，其中 θ 是陪集 $x+(x^n-1)$，证明：若 $a=\alpha_0+\alpha_1\theta+\cdots+\alpha_{n-1}\theta^{n-1}$，$\alpha_i\in\Phi$，则 a_R 的关于基 $(1,\theta,\cdots,\theta^{n-1})$ 的矩阵是**循环矩阵**

$$A=\begin{bmatrix}\alpha_0 & \alpha_1 & \cdots & \alpha_{n-1}\\ \alpha_{n-1} & \alpha_0 & \alpha_1\cdots & \alpha_{n-2}\\ \vdots & \vdots & \vdots & \vdots\\ \alpha_1 & \alpha_2 & \alpha_3\cdots & \alpha_0\end{bmatrix}.$$

证明：若 Φ 包含 1 的 n 个相异的 n 次根 ξ_i，则

$$N(a)=\det A=\prod_{j=1}^{n}\left(\sum_{0}^{n-1}\alpha_i\xi_j^i\right).$$

2. 设 $P\supseteq\Phi\supseteq E$ 是域 E 的有限维扩域，$a\in P$ 且 $x^n-\alpha_1x^{n-1}+\cdots+(-1)^n\alpha_n$ 是 a 在 Φ 上的最小多项式，因而(20)规定了 $\Phi(a)/\Phi$ 的一个矩阵表示。证明我们可通过下列方法得到 $\Phi(a)/E$ 的一个矩阵表示：将所出现的元 0，1 分别用 $h\times h$ 的零矩阵和单位矩阵代替，而 α_i 则用 Φ/E 的一个矩阵表示的表示矩阵 $\lambda(\alpha_i)$ 代替。利用拉普拉斯展开式验证结果矩阵的行列式是

$$N_{\Phi(a)|E}(a)=\det\lambda(\alpha_n).$$

由于 $\alpha_n=N_{\Phi(a)|\Phi}(a)$，此式给出：

$$N_{\Phi(a)|E}(a)=N_{\Phi|E}(N_{\Phi(a)|\Phi}(a)).$$

然后证明 $N_{P|E}(a)=N_{\Phi(a)|E}(a)^r$，$r=[P:\Phi(a)]$。利用这些结果证明 $\mathfrak{A}=P$ 时的公式(31)。

3. 设 $\mathfrak{A}/\Phi$ 是具有基 $(u_1,u_2,\cdots,u_n)$ 的一个代数，$\mathfrak{X}=\Phi(\xi_1,\xi_2,\cdots,\xi_n)$ 是含未定元 ξ_i 的有理式域，考虑 $\mathfrak{X}$ 上的代数 $(\mathfrak{A}\otimes_\Phi\mathfrak{X})$，它有 $\mathfrak{X}$ 上的基 $(u_1,u_2,\cdots,u_n)$，证明：若 $X=\sum_1^n\xi_iu_i$，则 X 的特征多项式 $f_X(x)$ 是 $\Phi[x,\xi_1,\cdots,\xi_n]$（$x$，$\xi_i$ 都是未定元）中的一个 n 次齐次多项式。利用此结果及卷 1 的中译本 pp.115－118

多项式环的算术理论证明X的最小多项式 $\mu_X(x)$ 有形式

$$x^m - t(\xi_1,\cdots,\xi_n)x^{m-1} + \cdots + (-1)^m n(\xi_1,\cdots,\xi_n),$$

这里 x^{m-i} 的系数是一个ξ的 i 次齐次多项式。若 $a = \Sigma\alpha_i u_i \in \mathfrak{A}$，作

$$\mu_a(x) = x^m - t(\alpha_1,\cdots,\alpha_n)x^{m-1} + \cdots + (-1)^m n(\alpha_1,\cdots,\alpha_n),$$

证明 $\mu_a(a) = 0$。

4. 各符号意义与题 3 相同并设 $\mathfrak{A} = \mathrm{P}$ 为一域，证明 $\mu_X(x)$是不可约的（提示：用§9 习题中的第 4 题）；由此证明 $f_X(x)$ 是 $\mu_X(x)$ 的一个幂；证明 $n(\xi_1,\cdots,\xi_n)$ 是不可约的而且其范数型 (norm form)

$$N(X) = \pm n(\xi_1,\cdots,\xi_n)^r.$$

15. 伽罗瓦上同调 人们总是喜欢研究一个有限维伽罗瓦扩张 P/Φ 的伽罗瓦群G到P内的或到P的非零元组成的乘群P^*内的映射。更一般地，我们经常遇到积集 $G\times G, G\times G\times G,\cdots$ 到P或P^*内的映射（G中的多元函数），一个特别重要类型的G到P^*内的映射 $s\to\mu_s\in\mathrm{P}^*$ 是一个满足伊米·诺特(Emmy Noether)方程

$$(61)\qquad \mu_{st} = \mu_s^t\cdot\mu_t$$

的映射。若 $\mu_s\in\Phi$，则 $\mu_s^t = \mu_s$，这可写成 $\mu_{st} = \mu_s\mu_t$。它恰是一个特征标或G到Φ内的可乘映射。若G是一个具有生成元g的循环群：$G = \{1, g, \cdots, g^{n-1}\}$，$g^n = 1$，则能使$N(\mu) = \mu\mu^g\cdots\mu^{g^{n-1}} = 1$ 的任意元 $\mu\in\mathrm{P}$ 定义一个满足(61) 的映射 $s\to\mu_s$，如果我们规定

$$(62)\qquad \mu_1 = 1,\ \mu_g = \mu,\ \mu_{g^2} = \mu\mu^g,\cdots,\ \mu_{g^{n-1}} = \mu\mu^g\cdots\mu^{g^{n-2}},$$

则 $\mu_{g^{i+1}} = \mu\mu^g\cdots\mu^{g^i} = (\mu\mu^g\cdots\mu^{g^{i-1}})^g\mu = \mu_{g^i}^g\mu_g$ 对$i = 1,\cdots,n-2$ 成立。对于 $i = 1$ 来说(61)是明显的，因为 $\mu_1 = 1$ 而且 $1 = \mu_{g^n} = \mu_{g^{n-1}}^g\mu_g = \mu^g\cdots\mu^{g^{n-1}}\mu = N(\mu)$。因此(61)对所有 $s = g^i$ 及 $t = g$ 成立。容易用归纳法检验它对一切s及一切 $t = g^j$ 也成立。

对于一般情况，若γ是P^*的任何元，我们可令 $\mu_s = \gamma(\gamma^s)^{-1}$，从而有

$$\begin{aligned}\mu_s^t\mu_t &= (\gamma(\gamma^s)^{-1})^t\gamma(\gamma^t)^{-1}\\ &= \gamma^t(\gamma^{st})^{-1}\gamma(\gamma^t)^{-1}\\ &= \gamma(\gamma^{st})^{-1}\end{aligned}$$

$$= \mu_{st}.$$

因此 $\mu_t = \gamma(\gamma^t)^{-1}$ 对于P中任何非零元 γ，满足诺特方程． 我们现在来证明诺特方程的这个“平凡”解是唯一可能的解，因为我们有

定理 19. 设 $s \to \mu_s$ 是 G 到 P^* 内的使 $\mu_{st} = \mu_s^t \mu_t (s, t \in G)$ 的一个映射，则在P中存在一个非零元 γ 使 $\mu_s = \gamma(\gamma^s)^{-1}$.

证 由于各 μ_s 是 $\neq 0$ 的及各自同构在P上是右线性无关的，可见算子 $\Sigma s\mu_s (\equiv \Sigma s \mu_s R)$ 是 $\neq 0$ 的．因此我们能找到一个 $\beta \in P$ 使 $\gamma \equiv \beta(\Sigma s \mu_s) = \Sigma \beta^s \mu_s \neq 0$．现在计算

$$\begin{aligned}
\gamma^t &= \left(\sum_{s \in G} \beta^s \mu_s\right)^t = \sum_s \beta^{st} \mu_s^t \\
&= \left(\sum_s \beta^{st} \mu_s^t \mu_t\right) \mu_t^{-1} \\
&= \left(\sum_s \beta^{st} \mu_{st}\right) \mu_t^{-1} \\
&= \left(\sum_s \beta^s \mu_s\right) \mu_t^{-1}
\end{aligned}$$

由于当 s 遍历 G 时，st 也遍历 G，故得所求的 $\gamma^t = \gamma \mu_t^{-1}$ 及 $\mu_t = \gamma(\gamma^t)^{-1}$.

我们已经看到，若 G 是具有生成元 g 的循环群，而且 μ 是P中范数为1的元 $(N_{P|\Phi}(\mu) = 1)$，则 $\mu_{g^i} = \mu\mu^g \cdots \mu^{g^{i-1}} (1 \leqslant i \leqslant n-1, \mu_1 = 1)$ 满足诺特方程．本定理断言存在一个 $\gamma \in P^*$ 使 $\mu = \mu_g = \gamma(\gamma^g)^{-1}$．这就得到下面的推论，它在一些文献中称为“希尔伯特定理 90”．

推论. 设 P/Φ 是一个有限维循环扩张域，g 是P在 Φ 上的伽罗瓦群的一个生成元，则任何使 $N_{P|\Phi}(\mu) = 1$ 的元 $\mu \in P$ 对于适当选择的 $\gamma \in P$ 都有形式 $\mu = \gamma(\gamma^g)^{-1}$.

刚才得到的两个结果对于伽罗瓦扩张 P/Φ 的加法群有类似的结果． 我们考虑 G 到P内的一个映射 $s \to \delta_s$，诺特方程的加群类比是

(63) $$\delta_{st} = \delta_s^t + \delta_t, \quad s, t \in G.$$

若 $\gamma\in P$，且令 $\delta_s=\gamma-\gamma^s$，则 $\delta_{st}=\gamma-\gamma^{st}$ 及

$$\delta_t^s+\delta_t=\gamma^s-\gamma^{st}+\gamma-\gamma^s=\delta_{st},$$

故(63)成立，因而定理 19 的直接类比成立：

定理 20. 设 $\delta_s(s\in G)$ 是 P 的满足 (63) 的元，则存在一个 $\gamma\in P$，使 $\delta_s=\gamma-\gamma^s$.

证　我们选择一个元 $\rho\in P$ 使 $T_{P|\Phi}(\rho)=\Sigma\rho^s\neq 0$. 根据戴得金无关定理有 $\sum\limits_{s\in G}s\neq 0$，所以这是能做到的. 令

$$\gamma=\sum_{s\in G}T(\rho)^{-1}\delta_s\rho^s,$$

则

$$\begin{aligned}\gamma-\gamma^t&=T(\rho)^{-1}\left(\sum_s(\delta_s\rho^s-\delta_s^t\rho^{st})\right)\\&=T(\rho)^{-1}\left(\sum_s(\delta_{st}\rho^{st}-\delta_s^t\rho^{st})\right)\\&=T(\rho)^{-1}\left(\sum_s\delta_t\rho^{st}\right)\\&=\delta_tT(\rho)^{-1}\left(\sum_s\rho^{st}\right)\\&=\delta_tT(\rho)^{-1}T(\rho)=\delta_t,\end{aligned}$$

这就是我们所要证明的.

对于循环群的情况，G 由 g 生成，条件 $N_{P|\Phi}(\mu)=1$ 的类比是 $T_{P|\Phi}(\mu)=0$. 若 μ 是这样的一个元，则可使 $\delta_1=0$，$\delta_{g^i}=\mu+\mu^g+\cdots+\mu^{g^{i-1}}$，容易检验(63)成立，我们因此有希尔伯特定理 90 的加群类比：

推论. 设 P/Φ 是有限维循环扩张，g 是 P/Φ 的伽罗瓦群的一个生成自同构，则任何使 $T_{P|\Phi}(\mu)=0$ 的元 $\mu\in P$ 对于一适当选择的 $\gamma\in P$ 有形式 $\gamma-\gamma^g$.

我们知道，若 P/Φ 是一个以 G 为其伽罗瓦群的有限维伽罗瓦扩域，则将 P 看作 Φ 上的向量空间时的线性变换集 $\mathfrak{L}_\Phi(P)$ 与具有形式 $\sum\limits_{s\in G}s\rho_s=\sum\limits_s s\rho_sR$ 的算子集 $\mathfrak{A}$ 重合（§4 引理）. 我们

也知道由戴得金无关定理，群元 $(s)(s\in G)$ 构成看作P上的右向量空间 $\mathfrak{L}_\Phi(\mathrm{P})$ 的一个基，我们现在来阐明诺特方程是由于考虑下列问题而产生的：环 $\mathfrak{L}_\Phi(\mathrm{P})$ 的哪些自同构能使子环 $\mathrm{P}_R(=1\mathrm{P})$ 的每个元不变？现设 A 是这样的一个自同构并令 $s^A=\mathfrak{U}_s(s\in G)$，则若将 A 作用到基本关系 $\rho_R s=s(\rho^s)_R$（方程 (2)）就可得到

$$\rho_R u_s=u_s(\rho^s)_R. \tag{64}$$

因此

$$\rho_R(s^{-1}u_s)=s^{-1}(\rho^{s^{-1}})_R u_s=s^{-1}u_s(\rho^{s^{-1}s})_R=(s^{-1}u_s)\rho_R.$$

故知 $s^{-1}u_s$ 是P的加群的一个自同态，它能与每个右乘变换 ρ_R 交换．由此推出 $s^{-1}u_s$ 本身是一个右乘变换（卷1的中译本 p.78），因此 $s^{-1}u_s=\mu_{sR}$，$u_s=s\mu_s(s\in G)$．我们现在利用 $s\to s^A=u_s$ 是 G 的一个同态这一事实，又可推出 $u_{st}=u_su_t(s,t\in G)$，因此我们有 $st\mu_{st}=(s\mu_s)(t\mu_t)=st\mu_s^t\mu_t$，故这个 $\mu_s\in\mathrm{P}^*$（因为 $\mu_s\neq 0$）满足诺特方程． 反之，如果倒转以上步骤我们就容易看到：若 $\mu_s\neq 0$ 满足诺特方程，则映射

$$A:\ \sum_s s\rho_s\to\sum_s u_s\rho_s,\ u_s=s\mu_s$$

是 $\mathfrak{L}_\Phi(\mathrm{P})$ 的一个自同构，它是 P_R 上的单位自同构． 我们知道 $\mathfrak{L}_\Phi(\mathrm{P})$的任何自同构，如果它是 Φ_R 上的单位自同构（在P中作用），那么它是一个内自同构（卷2的中译本 p.213 习题的第5题），因此存在一个元 $C\in\mathfrak{L}_\Phi(\mathrm{P})$ 使 $X^A=C^{-1}XC$ 对所有 $X\in\mathfrak{L}_\Phi(\mathrm{P})$ 成立．特别地，我们有 $\rho_R=\rho_R^A=C^{-1}\rho_RC$ 对所有 $\rho\in\mathrm{P}$ 成立，即 C 可与每个 ρ_R 交换；故可推得 $C=\gamma_R$，其中 γ 是P的一个非零元，此时

$$\begin{aligned}s\mu_s=u_s=s^A=C^{-1}sC=\gamma_R^{-1}s\gamma_R\\=s(\gamma^{-1})_R^s\gamma_R=s((\gamma^{-1})^s\gamma)_R,\ s\in G.\end{aligned}$$

由此推得 $\mu_s=\gamma(\gamma^s)^{-1}$．这就给出了定理19的另一证法．当然，这个证明不象第一个那样初等，但在前后文内容不便使用第一法时它还是非常有用的．

$\mathfrak{L}_\Phi(\mathrm{P})$ 看作 $\mathfrak{A}=\{\Sigma s\rho_s\}$ 的表示为我们提供了一类更一般的

环的构造法，这个环称为域 P 及其伽罗瓦群 G 的交叉积. 为此可考虑 P 上的一个右向量空间 $\mathfrak{B}$，它有基 (u_s) 与群 G 成 1－1 对应：$s \to u_s$，因此 $\mathfrak{B}$ 的元能且仅能以一种方式写成 $\sum_s u_s\rho_s(\rho_s \in \mathrm{P})$ 的形式，故 $[\mathfrak{B}:\mathrm{P}]_R = (G:1)$. 现设有 $G \times G$ 到 P^* 内的一个映射，它使每个群元的有序对 (s, t) 对应于 $\mu_{st} \in \mathrm{P}^*$，我们利用它们根据下列公式在 $\mathfrak{B}$ 中定义一个乘法：

$$(65) \qquad \left(\sum_{s \in G} u_s\rho_s\right)\left(\sum_{t \in G} u_t\sigma_t\right) = \sum_{s,t} u_{st}\rho_s^t\sigma_t\mu_{s,t}.$$

容易验证，这个乘法关于加法是(左，右)两方面可分配的，因此 $\mathfrak{B}$ 将成为一个环当且仅当乘法的结合律成立. 由于它适合分配律，所以只须对于 $a = u_s\rho$，$b = u_t\sigma$，$c = u_v\tau(s, t, v \in G)$ 有 $(ab)c = a(bc)$ 就足够了，现因

$$\begin{aligned}(ab)c &= (u_{st}\rho^t\sigma\mu_{s,t})(u_v\tau)\\ &= u_{stv}\rho^{tv}\sigma^v\tau\mu_{s,t}^v\mu_{st,v}\\ a(bc) &= (u_s\rho)(u_{tv}\sigma^v\tau\mu_{t,v})\\ &= u_{stv}\rho^{tv}\sigma^v\tau\mu_{s,tv}\mu_{t,v}.\end{aligned}$$

因此结合律成立当且仅当

$$(66) \qquad \mu^v_{s,t}\mu_{st,v} = \mu_{s,tv}\mu_{t,v}, \quad s, t, v \in G.$$

满足这些条件的非零元 $\mu_{s,t}(s, t \in G)$ 的集合称为一个 (G, P^*) **因子组**. 我们上面的讨论表明这样一个组由公式(65)定义一个环 $\mathfrak{B}$，结合性条件恰对应于条件(66). 这个环 $\mathfrak{B}$ 称为 G 与 P 的关于因子组 $\mu_{s,t}$ 的**交叉积**，我们记作 $\mathfrak{B} = (G, \mathrm{P}, \mu)$ 以指明它的要素 G, P 及因子组 $\mu = (\mu_{s,t})$.

如果仍将 $\mathfrak{L}_\Phi(\mathrm{P})$ 的表示看作 $\mathfrak{A} = \{\Sigma s\rho_s\}$，我们就知道 $\mathfrak{A}$ 同构于交叉积 $(G, \mathrm{P}, 1)$，这里 1 是因子组 $\mu_{s,t} = 1(s, t \in G$, 1 是 P 的单位元)，这只要将(65)与 $\mathfrak{A}$ 的元的乘法对比就清楚了. 我们现在将 $\mathfrak{A}$ 在 P 上的右基 (s) 用 (u_s) 代替，这里 $u_s = s\gamma_s$，而 γ_s 是 P 的一个非零元，则有

$$\begin{aligned}u_su_t &= (s\gamma_s)(t\gamma_t) = st\gamma_s^t\gamma_t\\ &= u_{st}\gamma_{st}^{-1}\gamma_s^t\gamma_t.\end{aligned}$$

因此我们知道$\mathfrak{A}$也同构于交叉积 (G, P, μ)，这里

$$(67) \qquad \mu_{s,t} = \gamma_{st}^{-1}\gamma_s^t\gamma_t.$$

容易检验它们满足因子组条件，但这却是不必要的，因为它们是等价于结合律的。由函数 $s \to \gamma_s \in \mathrm{P}^*$ 利用(67)得到的因子组μ称为等价于1 $(\mu \sim 1)$。我们所建立的结果是：若 $\mu \sim 1$，则 (G, P, μ) 同构于$\mathfrak{L}_\Phi(\mathrm{P})$。我们可能会猜想定理18的类比能对因子组有效，但是情况并不如此，我们将通过循环群的特殊情况来说明这点。

设G是一个以g为生成元的循环群，且设 $(G:1) = n$。我们设当 $0 \leqslant i, j \leqslant n-1$ 时，有

$$(68) \qquad \mu_{g^i,g^j} = \begin{cases} 1, & 若\ i+j<n \\ \alpha \neq 0\ (\in \Phi), & 若\ i+j \geqslant n. \end{cases}$$

我们要检验因子组条件(66)，由于1，$\alpha \in \Phi$，这些能简化为

$$(69) \qquad \mu_{g^i,g^j}\mu_{g^{i+j},g^k} = \mu_{g^i,g^{j+k}}\mu_{g^j,g^k}.$$

此时共有三种情况：$i+j+k<n$，$n \leqslant i+j+k<2n$ 及 $i+j+k \geqslant 2n$。在第一种情况，等式两端均化为1；在第二种情况，两端均为α；而在第三种情况，则两端均为α^2。若G是循环群而且μ是刚才所定义的类型，则交叉积 (G, P, μ) 称为循环代数或循环交叉积。条件 $\mu \sim 1$ 表示存在一些非零元 γ_{g^i} 使 $\mu_{g^i,g} = \gamma_{g^{i+1}}^{-1}\gamma_{g^i}^g\gamma_g$。这表明对于 $\gamma = \gamma_g$，$\gamma_{g^2} = \gamma\gamma^g$，$\cdots$，$\gamma_{g^{n-1}} = \gamma\gamma^g\cdots\gamma^{g^{n-2}}$ 来说，$\alpha = \gamma_1^{-1}\gamma_{g^{n-1}}^g\gamma = \gamma_1^{-1}\gamma\gamma^g\cdots\gamma^{g^{n-1}} = \gamma_1^{-1}N_{\mathrm{P}|\Phi}(\gamma)$。但 $1 = \mu_{1,1} = \gamma_1^{-1}\gamma_1^1\gamma_1$ 给出 $\gamma_1 = 1$，故必须有 $\alpha = N_{\mathrm{P}|\Phi}(\gamma)$。易知这个条件也可推出 $\mu \sim 1$。由此可知我们能够得到一个因子组 $\mu \nsim 1$，这只要选择一个元 $\alpha \in \Phi$，它不是P中任何元γ的范数就行了，例如取Φ为实数域而P是复数域，$\mathrm{P} = \Phi(i)$，$i^2 = -1$，则当 $\gamma = \gamma_1 + i\gamma_2 (\gamma_1, \gamma_2 \in \Phi)$ 时有 $\gamma^g = \bar{\gamma} = \gamma_1 - i\gamma_2$ 以及 $N(\gamma) = \gamma_1^2 + \gamma_2^2 \geqslant 0$。因此当 $\alpha < 0$ 时，α不是一个范数。这里要指出的是：由这样一个α构成的循环交叉积同构于Φ上的哈密顿 (Hamilton) 四元数代数。

我们讨论的以上各概念在群的上同调理论中全属特殊情况，我们将简明地概述其一般情况：我们从任一群G及整数环上的G的群环 $I(G)$ 开始，$I(G)$ 的元是元 $\sum_{s\in G} m_s s$，这里的 m_s 是整数，且对于G的一个有限子集来说 $m_s\neq 0$（参看卷1的中译本 p.89 习题 39 的第2题）。现规定：$\Sigma m_s s=\Sigma n_s s$当且仅当对于一切$s$都有 $m_s=n_s$；$I(G)$中的加法按分量相加进行：

$$\Sigma m_s s+\Sigma n_s s=\Sigma(m_s+n_s)s;$$

乘法则规定为 $\left(\sum_{s\in G} m_s s\right)\left(\sum_{t\in G} n_t t\right)=\sum_{s,t\in G} m_s n_t st$。由于$G$是可结合的，所以 $I(G)$ 是一个结合环。设 $\mathfrak{M}$ 是一个右 $I(G)$ 模，则 $\mathfrak{M}$ 在加法下是一个交换群，并且定义了乘积 $xa(x\in\mathfrak{M},\ a\in I(G),\ xa\in\mathfrak{M})$ 能使 $(x+y)a=xa+ya$，$x(a+b)=xa+xb$，$x(ab)=(xa)b, x1=1$。

令 $C^r(G,\mathfrak{M})$ 代表r重积 $G\times G\times\cdots\times G$ 到 $\mathfrak{M}$ 内的映射集，$C^r(G,\mathfrak{M})$ 的元称为G关于模 $\mathfrak{M}$ 的r上链，它们是映射 $(s_1,s_2,\cdots,s_r)\to f(s_1,s_2,\cdots,s_r)\in\mathfrak{M},\ (s_i\in G)$。如果按通常方法定义 $f+g$：$(f+g)(s_1,s_2,\cdots,s_r)=f(s_1,s_2,\cdots,s_r)+g(s_1,s_2,\cdots,s_r)$，我们就可将 $C^r(G,\mathfrak{M})$ 组成一个交换群。现在定义一个同态 d，称为 $C^r(G,\mathfrak{M})$ 到 $C^{r+1}(G,\mathfrak{M})$ 内的上边缘算子，为此对于 $C^r=C^r(G,\mathfrak{M})$ 中的f用如下的方法定义df：

$$(70)\qquad\begin{aligned}(df)(s_1,s_2,\cdots,s_{r+1})&=f(s_2,\cdots,s_{r+1})\\&+\sum_{i=1}^{r}(-1)^i f(s_1,\cdots,s_{i-1},s_i s_{i+1},\cdots,s_{r+1})\\&+(-1)^{r+1}f(s_1,\cdots,s_r)s_{r+1}.\end{aligned}$$

显然 $d(f+g)=df+dg$，故d是 C^r 到 C^{r+1} 内的一个同态。严格说来，我们应该将由(70)定义的d记作 d_r，但是用这同一符号表示所有这些定义在 $C^r(r=1,2,\cdots)$ 上的同态将更为方便。取模 $\mathfrak{M}$ 本身作为0上链群 C^0，并将 C^0 也包括进来是很方便的。这时若 $x\in C^0=\mathfrak{M}$，则 dx 是 C^1 的使 $(dx)s=x-xs$ 的元素。

将d（作用于 C^r 上）的核表为 Z^r，它的元称为G关于模 $\mathfrak{M}$

的 r 上循环. 在 d 下 C^{r-1} 在 C^r 内的象表为 B^r，它的元称为 r 上边缘. Z^r 及 B^r 都是 C^r 的子群而且可证 $Z^r \supseteq B^r$，这等价于证明：对于上边缘算子 d 有 $d^2 = 0$，我们把它的证明留作习题（下面习题中的第 1 题）. 商群 $H^r(G, \mathfrak{M}) = Z^r/B^r$ 称为G关于模$\mathfrak{M}$的第 r 个上同调群，这里我们取 $r = 0, 1, 2, \cdots$，并约定 $B^0 = 0$，因此 $H^0 = Z^0$，这里 Z^0 是 0 上循环的群，这个群的元恰好是 $\mathfrak{M}$ 的对所有 $s \in G$ 都有 $xs - x = 0$ 的元 x，显然它们恰是 $\mathfrak{M}$ 关于G的不变元集.

现在我们来阐明本节所考察的各概念是适合这种一般描述的. 今取G为有限维伽罗瓦扩张 P/Φ 的伽罗瓦群，对于模 $\mathfrak{M}$ 则可取 P 的乘群 P^* 或取 P 的加群 $(\mathrm{P}, +)$；在第一种情况我们利用如下规定的乘法 ρa 将 P^* 作成一个 $I(G)$ 模：

$$\rho a = \prod_{s \in G} (\rho^s)^{m_s} \quad \left(\rho \in \mathrm{P}^*, \quad a = \sum_{s \in G} m_s s\right).$$

由于G是一个有限群，我们是不难定义这个乘积的. 关于模的公理的检验是很平凡的，我们留给读者. 一个 1 上链 $s \to \mu_s = \mu(s) \in \mathrm{P}^*$ 是一个上循环当且仅当 $(d\mu)(s, t) = \mu_t \mu_{st}^{-1} \mu_s^t = 1$（$\mathrm{P}^*$ 的 0）；这等价于 $\mu_{st} = \mu_t \mu_s^t$，而这就是伊米 · 诺特方程 (61). 若 $\gamma \in \mathrm{P}^*$，则 γ 是一个 0 上链而且它的上边缘是 1 上链 $f(s) = \gamma(\gamma^s)^{-1}$. 定理 19 现在可改述为如下命题： G关于 P^* 的每个 1 上循环都是一个上边缘. 换言之，$Z^1/B^1 = 1$，或G关于 P^* 的第一个上同调群是恒等元群.

若 $(s, t) \to \mu_{s,t}$ 是一个 2 上链，则上边缘定义给出以下结果：

$$(d\mu)(s, t, u) = \mu_{t,u} \mu_{st,u}^{-1} \mu_{s,tu} (\mu_{s,t}^u)^{-1}.$$

由此推得 $\mu_{s,t}$ 是一个 2 上循环当且仅当 $\mu_{s,tu} \mu_{t,u} = \mu_{st,u} \mu_{s,t}^u$ ($s, t, u \in G$) 而这些恰是定义一个因子组的条件 (66). 因此各 2 上循环都恰是因子组. 若 $s \to \gamma_s$ 是一个 1 上链，它的上边缘 $d\gamma$ 由 $(d\gamma)(s, t) = \gamma_t (\gamma_{st})^{-1} \gamma_s^t$ 给出，因此各 2 上边缘都恰是等价于 1 的因子组. 经过一般考虑可得：因子组的集在乘法 $(\mu\nu)_{s,t} =$

$\mu_{s,t}\nu_{s,t}$ 下构成一个群；等价于1的因子组构成一子群，而第二个上同调群 $H^2(G, P^*)$ 是第一个群关于第二个群的商群。如我们所看到的，一般地，上同调群 $H^0(G, P^*)$ 是 P^* 的 G 不变元集，因此它是子域 Φ 的乘群 Φ^*.

对加法群 (P, +) 可以作完全类似的讨论，这时，借助于定义 $\rho a = \sum_{s\in G} m_s \rho^s$ 将加群 (P, +) 看作一个 $I(G)$ 模，易见定理20断言 G 关于 (P, +) 的第一个上同调群是 0. 可以证明：如果 P 的特征是 0 或者不是 G 的阶 n 的因子时，则所有上同调群 $H^r(G, P)=0$ $(r\geq 1)$，这是下面习题中第2题的直接结果。

习　题　16

1. 证明：$d^2=0$.

2. 设 G 是 n 阶有限群，$\mathfrak{M}$ 是一个 $I(G)$ 模，它在以下意义下是唯一 n 可除的：对于任何 $y\in\mathfrak{M}$，存在一个唯一的 x $\left(写成 \frac{1}{n}y\right)$ 使 $nx=y$. 证明：对于 $r\geq 1$，群 $H^r(G, \mathfrak{M})=0$.

3. 设 P/Φ 是一个循环扩张，$[P:\Phi]=n$，r 是 n 的一个因子，γ 是 Φ 的一个使 $\gamma^r=N_{P|\Phi}(\rho)$ $(\rho\in P)$ 的非零元. 证明 $\gamma=N_{E|\Phi}(\eta)$，这里 E/Φ 是 P/Φ 的使 $(P:E)=r$ 的(唯一的)子域，而且 $\eta\in E$.（提示：令 $n=mr$ 并考虑元 $\beta=\rho\rho^s\cdots\rho^{s^{m-1}}$，证明 $N_{P|E}(\beta)=\gamma^r$ 并对 $\beta^{-1}\gamma$ 应用希尔伯特定理 90).

16. 域的合成　本节所考虑的问题可粗略地描述如下：给定 Φ 上的两个扩张域 E 和 P 后，如何将它们结合起来以组成 Φ 的另一扩张域；简述之，我们将在以下精确定义中规定 Φ 上的 E 与 P 的合成域：

定义 3.　设 E 与 P 是 Φ 上的两个域，则 E/Φ 与 P/Φ 的一个合成域是一个三元组 (Γ, s, t)，这里的 Γ 是 Φ 上的一个域，s 和 t 分别是 E/Φ 和 P/Φ 到 Γ/Φ 内的同构，它们使 Γ 是由象 E^s 和 P^t 生成的一个域。E/Φ 和 P/Φ 的两个合成域 (Γ, s, t) 和 (Γ', s', t') 是等价的，如果存在一个 Γ/Φ 到 Γ'/Φ 上的同构 u 使 $su=s'$ 和 $tu=t'$.

现在的问题是确定合成域的等价类，我们将在它们中有一域

(例如 P)是Φ上的有限维扩张域这个前提下考虑本问题，到第四章 §10 才研究无限维扩张域的问题.

设 (Γ, s, t) 是 E/Φ 和 P/Φ 的一个合成域,其中 $[\mathrm{P}:\Phi]=n<\infty$，我们考虑子集

$$E^s\mathrm{P}^t=\left\{\sum_i \varepsilon_i^s\rho_i^t \middle| \ \varepsilon_i \in E,\ \rho_i \in \mathrm{P}\right\}.$$

显然这是 Γ/Φ 的两个子代数 E^s/Φ 和 P^t/Φ 生成的子代数. 还易证,如果 $(\rho_1, \rho_2, \cdots, \rho_n)$ 是 P/Φ 的一个基,则

$E^s\mathrm{P}^t=E^s\rho_1^t+E^s\rho_2^t+\cdots+E^s\rho_n^t$ 是 $\rho_i^t(1\leqslant i\leqslant n)$

的 E^s 线性组合集. 由于 Γ，从而 $E^s\mathrm{P}^t$ 是可换的，$E^s\mathrm{P}^t$ 是 E^s 上的一个代数而 $[E^s\mathrm{P}^t:E^s]\leqslant n<\infty$. 由于 $E^s\mathrm{P}^t$ 包含于一个域中，它没有零因子，因此由导言的 VII，$E^s\mathrm{P}^t$ 是一个域;由于 Γ 是由 E^s 及 P^t 生成的 Γ 的子域，故 $\Gamma=E^s\mathrm{P}^t$. 这个重要关系引导我们注意张量积代数 $E\otimes_\Phi \mathrm{P}$，对于它的元我们仍用原来的符号 $\Sigma\varepsilon_i\otimes\rho_i$ 表示. 张量积的基本性质是: 映射 $\Sigma\varepsilon_i\otimes\rho_i\to\Sigma\varepsilon_i^s\rho_i^t$ 是 $E\otimes_\Phi\mathrm{P}$ 到 $\Gamma=E^s\mathrm{P}^t$ 上的一个同态；若 $\mathfrak{J}$ 是这个同态的核，则 $\Gamma\cong(E\otimes_\Phi\mathrm{P})/\mathfrak{J}$. 由于 Γ 是一个域，由此推出 $\mathfrak{J}$ 是一个**极大理想**，即 $\mathfrak{J}$ 是 $E\otimes\mathrm{P}$ 的一个真子集而且不存在理想 $\mathfrak{J}'$ 使 $E\otimes\mathrm{P}\supset\mathfrak{J}'\supset\mathfrak{J}$. 反之,若 $\mathfrak{J}$ 是 $E\otimes\mathrm{P}$ 中的一个极大理想，则 $\Gamma=(E\otimes\mathrm{P})/\mathfrak{J}\neq 0$，这就是说它没有 $\neq 0$ 及 $E\otimes\mathrm{P}$ 的理想,由卷1的中译本 p.73 知 Γ 是一个域. 现在可给出以下结果:

定理 21. 设 E/Φ 及 P/Φ 是域且 $[\mathrm{P}:\Phi]<\infty$，$\mathfrak{J}$ 是 $E\otimes_\Phi\mathrm{P}$ 中的一个极大理想，s 是E到$\Gamma=(E\otimes\mathrm{P})/\mathfrak{J}$ 内的映射 $\varepsilon\to\varepsilon\otimes 1+\mathfrak{J}$，$t$ 是P到Γ内的映射$\rho\to 1\otimes\rho+\mathfrak{J}$，则 (Γ, s, t) 是 E/Φ 与 P/Φ 的一个域合成. $E\otimes\mathrm{P}$ 中不同的极大理想 $\mathfrak{J}$、$\mathfrak{J}'$ 在这种方法下产生不等价的合成域. 此外，E/Φ 与 P/Φ 的每个合成域等价于 $E\otimes\mathrm{P}$ 中的一个极大理想 $\mathfrak{J}$ 给出的一个 (Γ, s, t).

证 若 $\mathfrak{J}$ 是 $E\otimes\mathrm{P}$ 中的一个极大理想,则 $\varepsilon\to\varepsilon\otimes 1$ 是一个到 $E\otimes\mathrm{P}$ 内的同态,因此 $s:\varepsilon\to\varepsilon\otimes 1+\mathfrak{J}$ 是一个到 $\Gamma=(E\otimes\mathrm{P})/\mathfrak{J}$ 内的同态. 由于 $1\longrightarrow 1+\mathfrak{J}$ 及E是一个域,故 s 是一个同

构。同理 $t:\rho\to 1\otimes\rho+\mathfrak{J}$ 是 P/Φ 到 Γ 内的一个同构。Γ 的任何元有形式 $\Sigma\varepsilon_i\otimes\rho_i+\mathfrak{J}$ 而 $\varepsilon_i\otimes\rho_i+\mathfrak{J}=(\varepsilon_i\otimes 1+\mathfrak{J})(1\otimes\rho_i+\mathfrak{J})=\varepsilon_i^s\rho_i^t$；故 Γ 是由 E^s 及 P^t 生成的。Γ 也是一个域，这是因为 $\mathfrak{J}$ 是一个极大理想，因此 (Γ, s, t) 是一个合成域。

其次设 $\mathfrak{J}$ 及 $\mathfrak{J}'$ 是两个极大理想，(Γ, s, t)，(Γ', s', t') 是相应的合成域，并假设存在一个 Γ/Φ 到 Γ'/Φ 上的同构 u 使 $s'=su$，$t'=tu$。设 $\Sigma\varepsilon_i\otimes\rho_i\in\mathfrak{J}$，则由 s，t 的定义给出 Γ 内的关系 $\Sigma\varepsilon_i^s\rho_i^t=0$。应用 u 可得 $\Sigma\varepsilon_i^{s'}\rho_i^{t'}=0$，这表示 $\Sigma\varepsilon_i\otimes\rho_i\in\mathfrak{J}'$，故 $\mathfrak{J}\subseteq\mathfrak{J}'$。由于 $\mathfrak{J}$ 是极大理想，我们有 $\mathfrak{J}=\mathfrak{J}'$。这就证明了：若合成域 (Γ, s, t)，(Γ, s', t') 等价，则 $\mathfrak{J}=\mathfrak{J}_{\prime}$。

最后，设 (Γ', s', t') 是以任何方式构成的 E/Φ 与 P/Φ 的一个合成域，我们已经看到映射 $\Sigma\varepsilon_i\otimes\rho_i\to\Sigma\varepsilon_i^s\rho_i^t$ 是 $E\otimes\mathrm{P}$ 到 Γ' 上的同态，其核 $\mathfrak{J}$ 是 $E\otimes\mathrm{P}$ 中的一个极大理想，我们有 $\Gamma=(E\otimes\mathrm{P})/\mathfrak{J}$ 到 Γ' 上的诱导同构 $u:\Sigma\varepsilon_i\otimes\rho_i+\mathfrak{J}\to\Sigma\varepsilon_i^s\rho_i^t$，检验可知这是由 $\mathfrak{J}$ 定义的合成域 (Γ, s, t) 与 (Γ', s', t') 的一个等价关系。证毕。

我们已经在合成域的等价类集与张量积 $E\otimes_\Phi\mathrm{P}$ 中的极大理想组 $\{\mathfrak{J}\}$ 之间建立了一个双射，由于 $E\otimes_\Phi\mathrm{P}$ 可看作 E 上的一个有限维代数（见导言），由下列结果可推出 E/Φ 与 P/Φ 的合成域的等价类只能有有限多个。

定理 22. 一个具有单位元的有限维代数只能有有限多个不同的极大理想；若它们是 $\mathfrak{J}_1, \mathfrak{J}_2, \cdots, \mathfrak{J}_h$ 且 $\mathfrak{R}=\bigcap_1^h\mathfrak{J}_i$，则

$$\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{R}\cong\Gamma_1\oplus\Gamma_2\oplus\cdots\oplus\Gamma_h,$$

这里 $\Gamma_i=\mathfrak{A}/\mathfrak{J}_i$。

证 直和 $\Gamma_1\oplus\Gamma_2\oplus\cdots\oplus\Gamma_h$ 恰是 h 元组 $(\gamma_1, \gamma_2, \cdots, \gamma_h)$ $(\gamma_i\in\Gamma_i)$ 的集，其相等、加法与乘法均按分量相等、相加、相乘规定进行，显然直和的维数是各 Γ_i 的维数之和。现设 $\mathfrak{J}_1, \cdots, \mathfrak{J}_h$ 是任意不同的极大理想 $\mathfrak{B}=\Gamma_1\oplus\Gamma_2\oplus\cdots\oplus\Gamma_h(\Gamma_i=\mathfrak{A}/\mathfrak{J}_i)$。通过映射 $a\to(a+\mathfrak{J}_1, a+\mathfrak{J}_2, \cdots, a+\mathfrak{J}_h)$ 定义 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的一

个同态(此映射是一个同态是 .

$\mathfrak{I}_j = \mathfrak{I}_j$ 对每个 i 都成立的元素 a_1,

证明这个同态是一个满射. 首先证明 $\mathfrak{I}_1$

这些 $\mathfrak{I}_j$ 是不相同的极大理想, $\mathfrak{A} = \mathfrak{I}_1 + \mathfrak{I}_2$,
们相乘可得 $\mathfrak{A} = \mathfrak{A}^2 = \mathfrak{I}_1^2 + \mathfrak{I}_1\mathfrak{I}_3 + \mathfrak{I}_2\mathfrak{I}_1 + \mathfrak{I}_2\mathfrak{I}_3$
在假设我们已有 $\mathfrak{A} = \mathfrak{I}_1 + \mathfrak{I}_2 \cdots \mathfrak{I}_k$. 由于 $\mathfrak{A} = \mathfrak{I}_1$
样方法相乘可得 $\mathfrak{A} = \mathfrak{I}_1 + \mathfrak{I}_2\mathfrak{I}_3 \cdots \mathfrak{I}_{k+1}$. 因此我们有
$\mathfrak{I}_2 \cdots \mathfrak{I}_h$, 由此可得 $\mathfrak{A} = \mathfrak{I}_1 + (\mathfrak{I}_2 \cap \cdots \cap \mathfrak{I}_h)$, 因为 $\mathfrak{I}_2 \cdot$
$\mathfrak{I}_3 \cap \cdots \cap \mathfrak{I}_h$. 若 a 是 $\mathfrak{A}$ 的任一元, 则由上述关系得 $a = b$
(这里 $b \in \mathfrak{I}_1$, $c \in \mathfrak{I}_2 \cap \cdots \cap \mathfrak{I}_h$), 因此 c 在上述同态下的象是
$(c + \mathfrak{I}_1, c + \mathfrak{I}_2 \cdots, c + \mathfrak{I}_h) = (a + \mathfrak{I}_1, \mathfrak{I}_2, \cdots, \mathfrak{I}_h)$. 这表明:若
γ_1 是 Γ_1 的任一元, 则元 $(\gamma_1, 0, \cdots, 0)$ 是这个同态的象. 类似地,若 γ_i 是 Γ_i 的任一元,则 $(0, \cdots, 0, \gamma_i, 0, \cdots, 0)$ 必在象中,相加可知任意元 $(\gamma_1, \gamma_2, \cdots, \gamma_h)$ 必在象中, 因而此同态是满射. 很明显,若 $\mathfrak{I}_1, \mathfrak{I}_2, \cdots, \mathfrak{I}_h$ 是不同的极大理想,则维数

$$[\mathfrak{A}:\Phi] \geqslant \sum_1^h [\Gamma_i:\Phi],$$

这里 $\Gamma_i = \mathfrak{A}/\mathfrak{I}_i$. 由于每个 $[\Gamma_i:\Phi] > 0$, 因而 $\mathfrak{I}_i$ 的个数是有界的. 我们还曾见到,若 $\mathfrak{I}_1, \mathfrak{I}_2, \cdots, \mathfrak{I}_h$ 是不同的极大理想且 $\mathfrak{R} = \cap \mathfrak{I}_h$, 则 $\mathfrak{A}/\mathfrak{R} \cong \Gamma_1 \oplus \cdots \oplus \Gamma_h$.

我们还要在 $\mathrm{P} = \Phi(\theta)$ 是 Φ 的一个单代数扩张的假设下求得合成域的更为精确的信息: 设 $f(x)$ 是 θ 在 Φ 上的最小多项式,则 $(1, \theta, \theta^2, \cdots, \theta^{n-1})$ 是 P/Φ 的一个基且若

$$f(x) = x^n - \alpha_{n-1}x^{n-1} - \cdots - \alpha_0,$$

则 $\theta^n = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1}$. 现考虑 $E \otimes_\Phi \mathrm{P}$, 此代数的元能且仅能以一种方式写成 $\sum_0^{n-1} \varepsilon_i \otimes \theta^i (\varepsilon_i \in E)$. 我们利用定义 $\eta(\Sigma \varepsilon_i \otimes \theta^i) = \Sigma \eta\varepsilon_i \otimes \theta^i (\eta \in E)$ (参看导言)就可以将 $E \otimes_\Phi \mathrm{P}$ 看作 E 上的代数, 显然 $1 \otimes \theta$ 是 E 上的 $E \otimes_\Phi \mathrm{P}$ 的一个生成元而且

此元在E上的最小多项式是$f(x)$，因此$E\otimes_{\Phi}\mathrm{P}\cong E[x]/(f(x))$.此代数的各理想有形式$(p(x))/(f(x))$，这里的$p(x)$是$f(x)$的一个因子，而且这样的一个理想是极大的当且仅当$p(x)$是不可约的. 从而差代数$E[x]/(f(x))/((p(x))/(f(x)))$[1]同构于域$E[x]/(p(x))$.

最后假设P是Φ的一个有限维可分扩张域,则可知$\mathrm{P}=\Phi(\theta)$，这里的θ的最小多项式$f(x)$是不可约的和可分的. 可分性的导数判定法表明在$E[x]$中我们有分解式

$$f(x)=p_1(x)p_2(x)\cdots p_h(x),$$

其中$p_i(x)$是不可约的正次数多项式,且当$i\neq j$时$p_i(x)\neq p_j(x)$.由此可知共有h个不等价的Φ上的P与E的合成域，它们有形式(Γ_j,s_j,t_j)，这里$\Gamma_j\cong E[x]/(p_j(x))$. 再由导言§2习题中的第1题，$E\otimes_{\Phi}\mathrm{P}\cong E[x]/(f(x))\cong\Gamma_1\oplus\Gamma_2\oplus\cdots\oplus\Gamma_h$，而且

$$\sum_1^h[\Gamma_j:E]=[\mathrm{P}:\Phi],$$

我们有以下结果:

定理 23. 设P/Φ是有限维可分扩张域而E/Φ是一个任意的扩张域，若θ是P的一个本原元素且$f(x)$是它在Φ上的最小多项式，则合成域(Γ,s,t)与$f(x)$在$E[x]$中的不可约因子$p(x)$成1—1对应. 若$(\Gamma_j,s_j,t_j)(j=1,2,\cdots,h)$是$\mathrm{P}/\Phi$与$E/\Phi$的不等价合成域，则$[\mathrm{P}:\Phi]=\sum_{j=1}^h[\Gamma_j:E]$.

习 题 17

1.证明：若P/Φ是一个有限维伽罗瓦扩张，则P与它本身的合成域共有$n=[\mathrm{P}:\Phi]$个互不等价的；而且如果(Γ,s,t)是其中之一,则$\Gamma=\mathrm{P}^s=\mathrm{P}^t$. 利用此结果证明：$\mathrm{P}\otimes_{\Phi}\mathrm{P}\cong\mathrm{P}^{(1)}\oplus\mathrm{P}^{(2)}\oplus\cdots\oplus\mathrm{P}^{(n)}$，这里$\mathrm{P}^{(i)}\cong\mathrm{P}$.

2.设P是Φ上的有限维伽罗瓦扩张,E是Φ上的P的一个子域，证明：$\mathrm{P}\otimes_{\Phi}E\cong\mathrm{P}^{(1)}\oplus\mathrm{P}^{(2)}\oplus\cdots\oplus\mathrm{P}^{(m)}$，这里$\mathrm{P}^{(i)}\cong\mathrm{P}$且$m=[E:\Phi]$.

3.设P/Φ是有限维可分扩张，证明：如果1)E/Φ是纯不可分的，或2)$E=$

1) 原著中此处括号排错. ——译者注.

$\Phi(\xi_1, \xi_2, \cdots, \xi_n)$ 是含未定元 ξ_i 的有理分式域，那么 P/Φ 与 E/Φ 仅能有一个合成域(在等价的意义下).

4.今定义 r 个扩张域 $P_i/\Phi(1 \leqslant i \leqslant r)$ 的一个合成域 $(\Gamma, s_1, s_2, \cdots s_r)$ 为一域 Γ/Φ 及 P_i 到 Γ 内的同构 s_i，使得 Γ 是由子域 $P_i^{s_i}$ 生成的. P_i 的两个这样的合成域 $(\Gamma, s_1, \cdots, s_r)$，$(\Gamma', s'_1, \cdots, s'_r)$ 称为等价的，如果存在一个 Γ/Φ 到 Γ'/Φ 内的同构 u 使 $s'_i = s_i u(1 \leqslant i \leqslant r)$. 假设每个 P_i/Φ 都是有限维的，试将定理 21 推广到合成域 $(\Gamma, s_1, \cdots, s_r)$ 及张量积 $P_1 \otimes P_2 \otimes \cdots \otimes P_r$ 上并加以证明.

5.设 P/Φ 是有限维伽罗瓦扩张，$(s_1, s_2, \cdots, s_r)$ 是 P/Φ 的自同构的一个有序 r 元组，则 $(P, s_1, s_2, \cdots s_r)$ 是 P/Φ 的一个 r 重合成域. 证明: $(s_1, \cdots, s_r)$ 及 $(s'_1, \cdots, s'_r)$ 确定等价的合成域当且仅当 $s'_i = s_i u$ 是 P/Φ 的一个自同构. 设 $\mathfrak{J}(s_1, \cdots, s_r)$ 是与 $(P, s_1, \cdots, s_r)$ 相应的 $P \otimes P \otimes \cdots \otimes P$($r$ 个因子)中的理想，利用共有 $[P:\Phi]^{r-1}$ 个不同理想 $\mathfrak{J}(s_1, \cdots, s_r)$ 以及

$$(P \otimes \cdots \otimes P)/\mathfrak{J}(s_1, \cdots, s_r) \cong P$$

的事实证明 $\mathfrak{J}(s_1, \cdots, s_r)$ 是 $P^{(r)} \equiv P \otimes \cdots \otimes P$ 中的唯一的极大理想，而且 P/Φ 的每个 r 重合成域都等价于合成域 $(P, s_1, s_2, \cdots, s_r)$ 中的一个. 注意 $\mathfrak{J}(s_1, \cdots, s_r)$ 是 $P^{(r)}/\Phi$ 到 P/Φ 内的使

$$\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_r \longrightarrow \rho_1^{s_1} \rho_2^{s_2} \cdots \rho_r^{s_r}$$

的同态的核.

第　二　章

方程的伽罗瓦理论

本章将讨论伽罗瓦理论的古典应用：多项式方程 $f(x)=0$ 的根式解的伽罗瓦判定法．粗略地说，一个方程能用根式解是指它的根可由其系数通过有理运算和开方得到．其判定法是伽罗瓦继阿贝尔和努芬尼（Ruffini）证明了一般五次方程不能用根式解后给出的．为了给出根式解的判定法，伽罗瓦带头发展了他的理论，除了需要前章所讨论的（其讨论的规模远远超出方程论的范围)群与域的基本对应关系等理论外，还需要一些具有特殊性质的结果，它们包括割圆域、即 1 的根的域，以及“纯粹”扩张 $P=\Phi(\theta)$，这里有 $\theta^n=\alpha$ 属于 Φ．我们对这些域感兴趣还因为它们在方程论以外有用，对它们的详尽讨论将在下章进行，本章将局限在方程论所需要的知识的极小范围内．

1. 方程的伽罗瓦群　设 Φ 是一个域，$f(x)$ 是 $\Phi[x]$ 中的正次数首项系数为 1 的多项式，P/Φ 是 $f(x)$ 的一个分裂域，因此 $P=\Phi(\rho_1,\cdots,\rho_m)$ 而且在 $P[x]$ 中

$$f(x)=(x-\rho_1)^{e_1}(x-\rho_2)^{e_2}\cdots(x-\rho_m)^{e_m},$$

这里 ρ_i 是不同的元，e_i 是正整数．由于 ρ_i 是 P/Φ 的生成元，P/Φ 的任一自同构 s 完全被它在根的有限集 $R=\{\rho_1,\rho_2,\cdots,\rho_m\}$ 上的作用所决定．但是每个 ρ_i^s 仍为 $f(x)$ 的一个根，因此 $\rho_i^s\in R$，而且 s 对于 R 的限制 s_f 是这个有限集的一个置换．由此可知 P/Φ 的伽罗瓦群 G 的每个 s 确定 R 的一个置换 s_f．映射 $s\to s_f$ 是 G 到 R 的 1-1 映射的对称群 $S(R)$ 内一个同态．此外，若 $s\in G$ 有性质 $\rho_i^s=\rho_i(1\leqslant i\leqslant m)$，则在 $P=\Phi(\rho_1,\cdots,\rho_m)$ 中 $s=1$．因此，$s\to s_f$ 是 G 与对称群 $S(R)$ 的一个子群 $G_f=\{s_f\}$ 间的一个同构．在这个同构观点下，我们就可在研究方程 $f(x)=0$

时将注意力从群 G 转移到置换群 G_f 上去，据此我们给出以下结论

定义 1. 若 Φ 是一个域，$f(x)$ 是 $\Phi[x]$ 中的一个非零多项式，则方程 $f(x)=0$ 在 Φ 上的伽罗瓦群是一个分裂域 P/Φ 的伽罗瓦群 G 在 $f(x)=0$ 在 P 内的根集中所诱导的群 G_f.

由于任二分裂域都是同构的，因此 G_f 必被 Φ 及 $f(x)$ 所唯一确定.

为了方便，我们总是将 R 的置换 $\rho_i\to\rho_i'$ 与 $\{1,2,\cdots,m\}$ 的置换 $i\to i'$ 等同起来，利用这种方法我们就可将 G_f 看作 $\{1,2,\cdots,m\}$ 的置换的对称群 s_m 的一个子群，从现在开始我们将总这样做；此外我们还假设 $f(x)$ 有单根，即 $e_i=1$. 由此可知 P/Φ 是伽罗瓦扩张，因此我们在伽罗瓦群 G 的子群类与 P/Φ 的子域 E/Φ 类间有了基本的对应关系. 把此结果与 G 到 G_f 上的同构联合起来就可得到 G_f 的子群类与子域 E/Φ 类之间的一个 1—1 对应；我们把这个对应于 G_f 的子群 H_f 的子域 E/Φ 称为"H_f 的不变元域". 事实上，E/Φ 是对应于 H_f 的 G 的子群 H 的不变元的域. 另一方面，H_f 是 $f(x)=0$ 在子域 E 上的伽罗瓦群.

我们知道对称群 S_m 包含交代群 A_m 作为指数为 2 的一个不变子群，A_m 是偶置换的集，即能写成偶数多个对换 (ij) 之积的置换之集(见卷1的中译本 pp. 35,36). 若 G_f 是方程 $f(x)=0$ 在 Φ 上的伽罗瓦群，则 $G_f\cap A_m$ 是 G_f 中指数为 1 或 2 的一个子群. 现在给出 P/Φ 的对应子域的一个识别法. 这里假设特征不为 2 (特征 $=2$ 的情况见下面的习题中的第 1 题)，其结果如下:

定理 1. 设 Φ 是一个特征 $\neq 2$ 的域，$f(x)$ 是一个属于 $\Phi[x]$ 的没有重根的非零多项式，P/Φ 是 $f(x)$ 的一个分裂域，$\rho_1,\rho_2,\cdots,\rho_m$ 是它的根，G_f 是方程 $f(x)=0$ 的伽罗瓦群，并已作为 $\{1,2,\cdots,m\}$ 的一个置换群，则 $G_f\cap A_m$ 的不变元子域是 $\Phi(\Delta)$，这里

$$(1)\qquad \Delta=\prod_{i<j=1}^{m}(\rho_i-\rho_j).$$

证　我们回顾一下交代群的一个标准特性，为此可考虑环

$$\Phi[x_1, x_2, \cdots, x_m]$$

(x_i 为未定元)：若 $i \to i^\sigma$ 是 $1, 2\cdots, m$ 的一个置换，则我们有 $\Phi[x_1, x_2, \cdots, x_m]$ 在 Φ 上的使 $x_i^{A(\sigma)} = x_i^\sigma$ 的自同构 $A(\sigma)$（参看卷 1 的中译本 p.100 及导言）. 设 $X = \prod_{i<j}(x_i - x_j)$，则 $X^{A(\sigma)} = \chi(\sigma)X$，这里的 $\chi(\sigma) = 1$ 或 -1 视 σ 是偶置换或奇置换而定（参看卷 1 的中译本 p.102 习题 44 的第 2 题）. 现设 π 是 Φ 上的 $\Phi[x_1, x_2, \cdots, x_m]$ 到 P/Φ 内的同态，它使 $x_i^\pi = \rho_i (1 \leqslant i \leqslant m)$；又设 s 在 P/Φ 的伽罗瓦群中，s_f 是 ρ_i 的对应置换，则若将 π 应用到关系 $X^{A(s_f)} = \chi(s_f)X$ 上去，我们就可以得到 $\Delta^s = \chi(s_f)\Delta$，这里 Δ 由 (1) 式给出. 由于 $\Delta \neq 0$，可知 $\Delta^s = \Delta$ 当且仅当 $s_f \in G_f \cap A_m$，因此方程 $f(x) = 0$ 在 $\Phi(\Delta)$ 上的伽罗瓦群是 $G_f \cap A_m$. 由伽罗瓦对应可见，$\Phi(\Delta)$ 是 $G_f \cap A_m$ 的不变元的集.

我们已经看过，对于任何 $s \in G$，$\Delta^s = \pm\Delta$. 故若 $\delta = \Delta^2$，则对于一切 s 都有 $\delta^s = \delta$，因此 $\delta \in \Phi$. 我们还知道，定理的命题等价于断言方程 $f(x) = 0$ 在 $\Phi(\Delta)$ 上的伽罗瓦群是 $A_m \cap G$. 故有

推论. $f(x) = 0$ 在 Φ 上的伽罗瓦群是交代群的一个子群当且仅当 δ 是 Φ 的一个元的平方.

证　显然 $G_f \subseteq A_m$ 或 $G_f = G_f \cap A_m$ 的条件是 $\Phi(\Delta) = \Phi$. 若这成立，则 $\Delta \in \Phi$，而且 $\delta = \Delta^2$ 是 Φ 的一个元的平方；反之，若 $\delta = \alpha^2 (\alpha \in \Phi)$，则 $\delta = \Delta^2$ 给出 $\Delta = \pm\alpha \in \Phi$，因此

$$\Phi(\Delta) = \Phi.$$

我们知道，若 θ 是 Φ 上的一个可分代数元而且 $\theta_1 = \theta, \theta_2, \cdots, \theta_n$ 是 θ 在 $\Phi(\theta)$ 到它的正规闭包内的同构下的不同的象，则 $\delta = \prod_{i<j}(\theta_i - \theta_j)^2$ 是域 $\Phi(\theta)/\Phi$ 的一个判别式（参看 §1.14）. 若和前面一样 $f(x) = (x - \rho_1)(x - \rho_2)\cdots(x - \rho_m)$，则 $\delta = \Delta^2 = \prod_{i<j}(\rho_i - \rho_j)^2$ 称为多项式 $f(x)$ 的判别式或方程 $f(x) = 0$ 的判别式. 由对称多项式的基本定理（卷 1 的中译本

p.102)，δ 可表成一个

(2) $$f(x)=x^m-\alpha_1x^{m-1}+\alpha_2x^{m-2}-\cdots+(-1)^m\alpha_m$$

的系数的多项式，该多项式的系数在素域之中．现在我们介绍怎样才能作到这点．我们从范德蒙德公式开始：

(3) $$\begin{vmatrix} 1 & 1 & \cdots 1 \\ \rho_1 & \rho_2 & \cdots \rho_m \\ \cdots & \cdots & \cdots \\ \rho_1^{m-1} & \rho_2^{m-1} & \cdots\ \rho_m^{m-1} \end{vmatrix} = \prod_{i>j}(\rho_i-\rho_j).$$

平方可得

(4) $$\delta=\begin{vmatrix} m & \sigma_1 & \sigma_2 & \cdots & \sigma_{m-1} \\ \sigma_1 & \sigma_2 & \sigma_3 & \cdots & \sigma_m \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \sigma_{m-1} & \sigma_m & \sigma_{m+1} & \cdots & \sigma_{2m-2} \end{vmatrix}$$

这里 $\sigma_i=\rho_1^i+\rho_2^i+\cdots+\rho_m^i$．由于方幂之和能表成系数在素域中的 α_i 的多项式，式(4)将给出 δ 的同类的式子[1]

我们现在就 $m=2,3$ 的情况求 δ：

$m=2$．我们有 $f(x)=x^2-\alpha_1x+\alpha_2=(x-\rho_1)(x-\rho_2)$，故 $\sigma_1=\rho_1+\rho_2=\alpha_1$，$\rho_1\rho_2=\alpha_2$．因此

$$\sigma_2=\rho_1^2+\rho_2^2=(\rho_1+\rho_2)^2-2\rho_1\rho_2=\alpha_1^2-2\alpha_2.$$

公式(4)给出

(5) $$\delta=2\sigma_2-\sigma_1^2=\alpha_1^2-4\alpha_2.$$

$m=3$．此时

$$f(x)=x^3-\alpha_1x^2+\alpha_2x-\alpha_3=(x-\rho_1)(x-\rho_2)(x-\rho_3)$$

故 $\sigma_1=\rho_1+\rho_2+\rho_3=\alpha_1$，$\rho_1\rho_2+\rho_2\rho_3+\rho_1\rho_3=\alpha_2$，$\rho_1\rho_2\rho_3=\alpha_3$．因此

$$\sigma_2=\rho_1^2+\rho_2^2+\rho_3^2=(\rho_1+\rho_2+\rho_3)^2-2(\rho_1\rho_2+\rho_1\rho_3+\rho_2\rho_3)$$
$$=\alpha_1^2-2\alpha_2.$$

要计算 σ_3 和 σ_4 可利用关系 $\rho_k^3=\alpha_1\rho_k^2-\alpha_2\rho_k+\alpha_3$，$\rho_k^4=\alpha_1\rho_k^3-$

---

1) 这可由对称多项式基本定理(卷 1 的中译本 p.102)算出．称为牛顿恒等式的显递归公式 (*explicit recursion formula*) 可将 σ_i 用 α_j 表出（卷 1 的中译本 p. 102 习题 44 的第 4 题）．

$\alpha_2\rho_k^2 + \alpha_3\rho_k$. 故

$$\begin{aligned}\sigma_3 &= \rho_1^3 + \rho_2^3 + \rho_3^3\\ &= \alpha_1(\rho_1^2 + \rho_2^2 + \rho_3^2) - \alpha_2(\rho_1 + \rho_2 + \rho_3) + 3\alpha_3\\ &= \alpha_1(\alpha_1^2 - 2\alpha_2) - \alpha_2\alpha_1 + 3\alpha_3\\ &= \alpha_1^3 - 3\alpha_1\alpha_2 + 3\alpha_3.\end{aligned}$$

$$\begin{aligned}\sigma_4 &= \alpha_1\sigma_3 - \alpha_2\sigma_2 + \alpha_3\sigma_1\\ &= \alpha_1(\alpha_1^3 - 3\alpha_1\alpha_2 + 3\alpha_3) - \alpha_2(\alpha_1^2 - 2\alpha_2) + \alpha_3\alpha_1\\ &= \alpha_1^4 - 4\alpha_1^2\alpha_2 + 4\alpha_1\alpha_3 + 2\alpha_2^2.\end{aligned}$$

应用(4)及以上各公式可得

$$(6)\qquad \begin{aligned}\delta &= 3\sigma_2\sigma_1 + 2\sigma_1\sigma_2\sigma_3 - \sigma_2^3 - 2\sigma_3^2 - \alpha_1^3\sigma_4\\ &= -4\alpha_1^3\alpha_3 + \alpha_1^2\alpha_2^2 + 18\alpha_1\alpha_2\alpha_3 - 4\alpha_2^3 - 27\alpha_3^2.\end{aligned}$$

其次,我们来求 $f(x)$ 在 $\Phi[x]$ 中不可约的一个判定法,这个判定法是基于将 G 作为 $\{1, 2, \cdots, m\}$ 的置换群之上的.

定理 2. 设 $f(x)\in\Phi[x]$ 在它的分裂域 P 中无重根,则 $f(x)$ 在 $\Phi[x]$ 中不可约当且仅当 $f(x) = 0$ 在 Φ 上的伽罗瓦群 G_f 是一个可迁置换群[1].

证 我们知道,一集M的一个变换群称为可迁的,如果对于任给的元素对 (x, y), $(x, y \in M)$, 在该群中总存在一个 σ 使 $x^\sigma = y$. 首先假设 $f(x)$ 在 $\Phi[x]$ 中是不可约的, ρ_1, ρ_2 是它在 P 中的两个根,由于 $f(x)$ 是不可约的以及 $f(\rho_1) = 0 = f(\rho_2)$, 存在 $\Phi(\rho_1)/\Phi$ 到 $\Phi(\rho_2)/\Phi$ 上的一个同构将 ρ_1 映射到 ρ_2 上. 此同构可扩张成 P/Φ 的一个自同构 s, 则 $s \in G$而且 $\rho_1^s = \rho_2$. 这推得 G_f 是可迁的. 反之,假设 G_f 是可迁的,并令 $f_1(x)$ 是 $f(x)$ 的一个不可约因子,它是正次数的而且 ρ_1 是它的一个根. 设 ρ_2是 $f(x)$ 的任意根,则存在一个 $s \in G$使 $\rho_1^s = \rho_2$, 故

$$f_1(\rho_2) = f_1(\rho_1^s) = f_1(\rho_1)^s = 0.$$

这表示 $f(x)$ 的每个根都是 $f_1(x)$ 的根,故 $f(x) = f_1(x)$ 是不可约的.

---

1) *Transitive permutation group*, 本书中译本前两卷译为传递置换群. ——译者注.

我们所得到的两个结果使我们在计算二、三次方程的伽罗瓦群时容易了，类似的想法可用于四次方程．我们先看前两种情况并在下面的习题中指出如何处理四次的情况．我们假设 Φ 的特征不为 2 且 $f(x)$ 有不同的根，若 $f(x)$ 是二次的，$f(x) = x^2 - \alpha_1 x + \alpha_2$，则它的群视 $\delta = \alpha_1^2 - 4\alpha_2$ 是或不是 Φ 中的一个元的平方而是 $A_2 = 1$ 或对称群 S_2．次令 $f(x) = x^3 - \alpha_1 x^2 + \alpha_2 x - \alpha_3$，若在 $\Phi[x]$ 中，$f(x) = (x - \rho)g(x)$，则 $f(x) = 0$ 的伽罗瓦群与二次式 $g(x)$ 的相同；因此可假设 $f(x)$ 在 $\Phi[x]$ 中不可约，由于 S_3 的唯一可迁子群是 S_3 和 A_3，伽罗瓦群 G_f 是它们中的一个。定理 1 的推论表明：如果

$$\delta = -4\alpha_1^3\alpha_3 + \alpha_1^2\alpha_2^2 + 18\alpha_1\alpha_2\alpha_3 - 4\alpha_2^3 - 27\alpha_3^2$$

是 Φ 中的一个元的平方，则 $G_f = A_3$，否则 $G_f = S_3$。

习　　题　　18

1．设 Φ 有特征 2 而且 $f(x) \in \Phi[x]$ 在它的分裂域 P 中有不同的根 $\rho_1, \rho_2, \cdots, \rho_m$．使 $\Delta' = \sum_{\sigma \in A_m} \rho_{1^\sigma}^{n-1} \rho_{2^\sigma}^{n-2} \cdots \rho_{(n-1)^\sigma}$．证明 $G_f \cap A_m$ 的不变元子域是 $\Phi(\Delta')$．

2．设 Φ 是一个有限域，$f(x)$ 是系数在 Φ 中的 n 次不可约多项式，证明 G_f 由一个 n 循环的各方幂构成，从而此循环可取为$(1\,2\,3 \cdots n)$．

在以下各题中均假设基域 Φ 的特征 $\neq 2$，$f(x) = x^4 - \alpha_1 x^3 + \alpha_2 x^2 - \alpha_3 x + \alpha_4$ 在分裂域 P/Φ 中有不同的根 $\rho_1, \rho_2, \rho_3, \rho_4$；$G$ 为 P/Φ 的伽罗瓦群．

3．证明子群 V（克莱因四元群 *Klein's Vierergruppe*）$= \{1, (12)(34), (13)(24), (14)(23)\}$ 是 S_4 的不变子群．

4．证明关于 $G_f \cap V$ 为不变元的子域是 $\Phi(\tau_1, \tau_2, \tau_3)$，这里

$$\tau_1 = \rho_1\rho_2 + \rho_3\rho_4,\ \tau_2 = \rho_1\rho_3 + \rho_2\rho_4,\ \tau_3 = \rho_1\rho_4 + \rho_2\rho_3.$$

5．设 $g(x) = (x - \tau_1)(x - \tau_2)(x - \tau_3)$（**$f(x)$ 的三次预解式**），验证

$$g(x) = x^3 - \beta_1 x^2 + \beta_2 x - \beta_3, \tag{7}$$

其中

$$\beta_1 = \alpha_2,\ \beta_2 = \alpha_1\alpha_3 - 4\alpha_1,\ \beta_3 = \alpha_1^2\alpha_4 + \alpha_3^2 - 4\alpha_2\alpha_4; \tag{8}$$

而且 $g(x)$ 与 $f(x)$ 有相同的判别式．

6．证明 S_4 的可迁子群是：(i) S_4，(ii) A_4，(iii) V，(iv) $C = \{1, (1234), (13)(24), (1432)\}$ 以及它的共轭子群，(v) $D = V \cup \{(12), (34), (1423), (1324)\}$ 即西罗 (Sylow) 2 群(阶为 8 的子群)及它的共轭子群．

7．证明 $g(x) = 0$ 的伽罗瓦群 G_g 同构于 $G_f/(G_f \cap V)$．设 $f(x)$ 不可约，试检验：

若 (i) $G_f = S_4$，则 G_g 的阶为 6，

(ii) $G_f = A_4$，则 G_g 的阶为 3，

(iii) $G_f = V$，则 $G_g = 1$，

(iv) $G_f = C$ 或其一共轭子群(即 S_4 的任一 4 阶循环子群)，则 G_g 的阶为 2，

(v) $G_f = D$ 或其一共轭子群(S_4 中任一 8 阶西罗 Sylow 子群)，则 G_g 的阶为 2.

注意这些结果除 G_f 在 (iv) 或 (v) 之一的情况外，都能使我们由 G_g 辨识出 G_f.

8. 证明：若 G_f 的阶为 2，则 $G_f \cong D$ 或 $G_f \cong C$ 视 $f(x)$ 在 $\Phi(\sqrt{\delta})$ 中是否不可约多项式而定，这里 δ 是 $f(x)$ 的判别式.

9. 确定 $x^4 + 3x^3 - 3x - 2 = 0$ 在有理数域上的伽罗瓦群.

2. 纯方程 本节将导出伽罗瓦判定法所需要的特殊结果，我们将用分裂域而不象前节那样用方程的群来表达这些结果的不变形式，我们所需要的结果涉及 $x^n - \alpha = 0$ (或 $x^n = \alpha$) 形的方程，它们称为纯方程(或二项方程). 有时我们使用记号 $\rho = \sqrt[n]{\alpha}$ 或 $\rho = \alpha^{1/n}$ 表示 ρ 是 $x^n = \alpha$ 的一个根. 我们先考虑 $\alpha = 1$ 的情形，$x^n = 1$ 的各根称为 1 的 n 次根(或 n 次单位根)，这个方程的一个分裂域 P 称为 Φ 上的 n 阶割圆域. 导数 $(x^n - 1)' = nx^{n-1}$ 与 $x^n - 1$ 不互素当且仅当其特征 $p \neq 0$ 且 $p|n$. 因此我们可写成 $n = p^e n'$，$(n', p) = 1$ 而且有 $x^n - 1 = (x^{n'} - 1)^{p^e}$. 所以 n 阶割圆域与 n' 阶割圆域重合. 我们从现在起每逢特征 $p \neq 0$ 的场合均假设 $p \nmid n$.

设 P/Φ 是 Φ 上的一个 n 阶割圆域，由于我们对于特征的规定，n 次单位根的集 $Z(n) = \{\zeta_i\}$ 包含 n 个元. 若 $m|n$，则由 $\eta^m = 1$ 可推得 $\eta^n = 1$；因此 n 阶割圆域包含所有的 m 阶割圆域，这里的 m 是 n 的约数，其次我们还可看到 $Z(n)$ 是 P 的乘法半群的一个子群，这是很明显的，因为由 $\zeta_1^n = 1 = \zeta_2^n$ 可推得

$$(\zeta_1\zeta_2)^n = 1, \ (\zeta_1^{-1})^n = 1.$$

由于 $Z(n)$ 是有限群，可见这是一个循环群(§1.13 引理1)，因此存在一个 $\zeta \in Z(n)$ 使 $Z(n) = \{\zeta^i | i = 0, 1, \cdots, n-1\}$. 这样的一个 ζ 称为本原 n 次单位根，由于 P/Φ 由 ζ_i 生成，我们又有 $P = \Phi(\zeta)$，故 ζ 是域 P/Φ 的一个本原元，我们现在来证明

定理 3. 若 Φ 的特征不是 n 的因子 (可以包括特征 0 的情况

在内)，则 n 阶割圆域 P/Φ 的伽罗瓦群 G 同构于 $I/(n)$ 中单位的乘群 $U(n)$ 的一个子群，这里的 I 是整数环.

证 和 §1 一样，用 G_f 表示由 G 导出的根集 $Z(n)$ 的置换群，由于 G_f 的元是自同构的限制，显然它们是 $Z(n)$ 的乘群的自同构，因此 $G_f(\cong G)$ 同构于 $Z(n)$ 的自同构群的一个子群. 今 $Z(n)$ 是一个 n 阶循环群，我们知道这样一个群的自同构群同构于 $U(n)$（卷 1 的中译本 p.46 习题 19 的第 3 题及 p.77 习题 36 的第 1 题)，因此伽罗瓦群 G 同构于 $U(n)$ 的一个子群.

值得注意的是 G 为可换群，因为 $U(n)$ 是可换群. 此外，我们还看到，若 l 是一个素数，则 $U(l)$ 恰是域 $I/(l)$ 的 ($l-1$ 阶) 乘群，我们知道，这是一个循环群，因此同构于 $U(l)$ 的一个子群的群 G 是循环群. 故有

推论. 若符号如定理 3 所示，则 G 是可换群而且当 n 是一个素数时 G 是循环群.

其次我们在假设基域 Φ 包含 n 个不同的 n 次单位根的前提下考虑任一纯方程 $x^n=\alpha$ 的伽罗瓦群，我们已经知道这时域的特征不是 n 的一个因子，因此若 $\alpha\neq 0$，则 $x^n-\alpha$ 与它的导数 nx^{n-1} 互素，故 $x^n-\alpha$ 有 n 个不同的根（在 $\alpha=0$ 的场合更简单)，我们有如下结论

定理 4. 若 Φ 包含 n 个不同的 n 次单位根，则方程 $x^n=\alpha$ 在 Φ 上的伽罗瓦群是一个循环群，其阶是 n 的一个因子.

证 设 P/Φ 是 $x^n-\alpha$ 在 Φ 上的一个分裂域，G 是它的伽罗瓦群，我们需要证明 G 是循环群. 若 $\alpha=0$，我们有 $P=\Phi$，$G=1$. 因此我们假设 $\alpha\neq 0$，设 ρ 是 $x^n-\alpha$ 在 P 中的一个根，若 $Z(n)=\{\zeta_1=1,\zeta_2,\cdots,\zeta_n\}$ 是包含于 Φ 中的 n 次单位根集，则可知 $Z(n)$ 在乘法下是一个循环群；又因 $\rho\neq 0$，显然 $\{\rho\zeta_1,\rho\zeta_2,\cdots,\rho\zeta_n\}$ 是 $x^n-\alpha$ 的根集，很明显，$P=\Phi(\rho)$；因此，一个自同构 $s\in G$ 完全由它在 ρ 上的作用所决定. 我们有 $\rho^s=\zeta_{i(s)}\rho$，这里的 $\zeta_{i(s)}$ 是 $\zeta\in Z(n)$ 中的一个，且被 s 唯一确定. 若 $t\in G$ 且 $\rho^t=\zeta_{i(t)}\rho$，则

$$\rho^{st} = \zeta_{i(t)}\rho^{s} = \zeta_{i(s)}\zeta_{i(t)}\rho.$$

这表示映射 $s \to \zeta_{i(s)}$ 是 G 到 $Z(n)$ 内的一个同态．若 $\zeta_{i(s)} = 1$，我们有 $\rho^s = \rho$，因此 $s = 1$，故 $s \to \zeta_i(s)$ 是一个同构．这就是说，G 与循环群 $Z(n)$ 的一个子群同构，定理由此得证．

我们证明伽罗瓦判定法还需要另一特殊结果，这就是定理 4 的下列逆定理．

定理 5. 假设 Φ 有 n 个不同的 n 次单位根，而且 P/Φ 是一个循环 n 维扩张域，则 $\mathrm{P} = \Phi(\xi)$，这里的 $\xi^n = \alpha \in \Phi$．

证　对 P 的假设是：P/Φ 是一个具有 n 阶循环伽罗瓦群 G 的伽罗瓦扩张，由于 P 是 Φ 上的可分域，它有一个本原元，故 $\mathrm{P} = \Phi(\theta)$．设 s 是 G 的一个生成元，而 ξ 是“拉格朗日预解式”(Lagrange resolvent)：

$$\xi = \theta + \theta^{s}\zeta^{-1} + \theta^{s^2}\zeta^{-2} + \cdots + \theta^{s^{n-1}}\zeta^{-(n-1)}, \tag{9}$$

这里 ζ 是一个本原 n 次单位根，则

$$\begin{aligned}\xi^s &= \theta^s + \theta^{s^2}\zeta^{-1} + \cdots + \theta\zeta^{-(n-1)} \\ &= \zeta(\theta + \theta^s\zeta^{-1} + \cdots + \theta^{s^{n-1}}\zeta^{-(n-1)}) = \zeta\xi.\end{aligned}$$

因此 $\xi^{s^k} = \zeta^k\xi$，所以 ξ 有 n 个不同的共轭元而且其最小多项式的次数为 n，故 $\mathrm{P} = \Phi(\xi)$．令 $\xi^n = \alpha$，则 $(\xi^n)^s = (\zeta\xi)^n = \xi^n$ 可推出 $\alpha^s = \alpha$，故 $\alpha \in \Phi$．于是定理得证．

习　题　19

1. 设 p 是一个不等于域 Φ 的特征的素数，证明：若 $\alpha \in \Phi$，则 $x^p - \alpha$ 在 $\Phi[x]$ 中不可约或者在这个域中有一个根．

2. 设 Φ 是有理数域，p 是一个素数，$x^p - \alpha$ 在 $\Phi[x]$ 中不可约，证明：方程 $x^p = \alpha$ 在 Φ 上的伽罗瓦群同构于 $I/(p)$ 中的形如 $y \to \gamma y + \delta (\gamma \neq 0)$ 的变换群．

3. 设 Φ 是一个特征 $p \neq 0$ 的域，证明：如果 $\alpha \neq \beta^p - \beta$ (β 在 Φ 中)，则 $x^p - x - \alpha$ 在 $\Phi[x]$ 中是不可约的．还证明：若 $x^p - x - \alpha$ 不可约，则方程 $x^p = x + \alpha$ 的群是 p 阶循环群(提示：可以检验，若 ρ 是 $x^p - x - \alpha = 0$ 的一个根，则 $\rho, \rho + 1, \rho + 2, \cdots, \rho + (p-1)$ 都是根；由此证明，这方程的伽罗瓦群同构于 $I/(p)$ 的加群的一个子群)．

4. 设 Φ 的特征 $p \neq 0$，P/Φ 是循环 p 维扩张域，证明：P 可在 Φ 上由一个使 $\xi^p - \xi = \alpha \in \Phi$ 的元素 ξ 生成．

3. 可用根式解的伽罗瓦判别法 我们首先需要精确给出一个方程 $f(x)=0$ 在一个域 Φ 上可用根式解的定义，现在给出下列

定义 2. 设 Φ 是一个域，$f(x)\in\Phi[x]$ 是正次数多项式，则方程 $f(x)=0$ 称为在 Φ 上能用根式解，如果分裂域 P/Φ 能够嵌入一个具有一个子域塔

$$\Phi=\Phi_1\subseteq\Phi_2\subseteq\Phi_3\subseteq\cdots\subseteq\Phi_{r+1}=\Sigma \tag{10}$$

的域 Σ 之中，这里的每个 $\Phi_{i+1}=\Phi_i(\xi_i)$ 而 $\xi_i^{n_i}=\alpha_i\in\Phi_i$. 这样的域链(10)[1]称为 Σ/Φ 的一个根塔.

为了简单，我们将限制域的特征为 0，这样就可以避免不可分性的复杂性以及 1 的根在特征 $p\neq 0$ 的场合的某些困难，我们的目的是建立以下的伽罗瓦判定法：

方程 $f(x)=0$ 在特征为 0 的域 Φ 上能用根式解当且仅当它的伽罗瓦群是可解的.

我们知道：一个群 G 是可解的是指它有一个子群链

$$G=G_1\supseteq G_2\supseteq G_3\supseteq\cdots\supseteq G_{r+1}=1$$

使每个 G_{i+1} 是 G_i 中的不变子群而且 G_i/G_{i+1} 是可换的. 可解群的每个子群及它的同态象都是可解的；此外，若 G 包含一个不变子群 H 使得 H 及 G/H 都是可解群，则 G 也是可解群；一个有限群 G 是可解的当且仅当它有一个合成群列 $G=G_1\supset G_2\supset\cdots\supset G_{s+1}=1$，它们的合成因子 G_i/G_{i+1} 是素数阶循环群. 我们还知道，交代群 A_n 当 $n\geqslant 5$ 时是单群，由这可知 n 个文字的对称群 S_n 当 $n\geqslant 5$ 时不是可解群. 关于 A_n 的这个命题的证明已在卷 1(中译本 p. 129)中给出，我们所说的其它结果则是正规群列理论的简单推论，它们中的大部分已在卷 1(中译本 p.129 及 p. 133)作为习题给出，我们假设读者已掌握了这些结果.

为了证明伽罗瓦判定法的必要性，我们还需要下面的

引理. 若 Σ 在特征为 0 的 Φ 上有一个根塔，则 Σ 有一个扩张域 Ω，它是 Φ 上的有限维伽罗瓦扩张，而且还有一个 Φ 上的根塔.

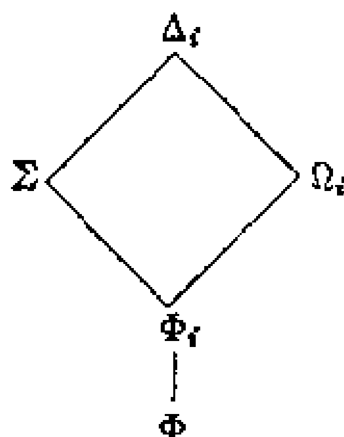
---

1) 原书误为(2). ——译者注

证　已知 $\Phi=\Phi_1\subseteq\Phi_2\subseteq\cdots\subseteq\Phi_{r+1}=\Sigma$，这里

$$\Phi_{i+1}=\Phi_i(\xi_i),\ \xi_i^{n_i}=\alpha_i\in\Phi_i.$$

我们将证明存在一个域 $\Delta_i\supseteq\Sigma$，它仍包含一个子域 Ω_i 使1) $\Omega_i\supseteq\Phi_i$，2) Ω_i 是 Φ 上的伽罗瓦扩张，3) Ω_i 在 Φ 上有一个根塔



对于 $i=1$，我们取 $\Delta_1=\Sigma$，$\Omega_1=\Phi_1$，并且假设对于一个固定的 i 给出了 Δ_i 与 Ω_i，使 G_i 为 Ω_i 在 Φ 上的伽罗瓦群，$\alpha_i^{s_1}$，$\cdots$，$\alpha_i^{s_k}$ 是元 α_i 在自同构 $s_j\in G_i$ 下的共轭元. 令

$$g_i(x)=\prod_{j=1}^{k_i}(x^{n_i}-\alpha_i^{s_j}),$$

则 $g_i(x)\in\Phi[x]$. 设 Δ_{i+1} 是 $g_i(x)$ 在 Δ_i 上的一个分裂域而且 $\xi_i,\xi_i',\xi_i'',\cdots$是 $g_i(x)$ 在 Δ_{i+1} 中的根，注意这些根中有一个是使 $\Phi_{i+1}=\Phi_i(\xi_i)$ 的 ξ_i，因为 $g_i(\xi_i)=0$ 且 $\Delta_{i+1}\supseteq\Delta_i\supseteq\Sigma$. 令 $\Omega_{i+1}=\Omega_i(\xi_i,\xi_i',\xi_i'',\cdots)$，由于 Ω_i/Φ 是一个多项式 $f_i(x)\in\Phi[x]$ 的一个分裂域，Ω_{i+1}/Φ 是 $f_i(x)g_i(x)$ 的一个分裂域. 又由于域的特征为0，Ω_{i+1} 是 Φ 上的伽罗瓦扩张. 因为 $\Omega_{i+1}\supseteq\Omega_i$ 及 $\xi_i\varepsilon\Omega_i$，$\Omega_{i+1}\supseteq\Phi_{i+1}=\Phi_i(\xi_i)$. 设 $\xi_i^{(h)}$ 是元 $\xi_i,\xi_i',\xi_i'',\cdots$中的任一个，则 $g_i(\xi_i^{(h)})=0$ 和 $g_i(x)=\Pi(x^{n_i}-\alpha_i^{s_j})$ 表示 $(\xi_i^{(h)})^{n_i}$ 是 $\alpha_i^{s_j}$ 中的一个，因此 $\Omega_{i+1}=\Omega_i(\xi_i,\xi_i',\xi_i'',\cdots)$ 在 Φ 上有一根塔. 这表示 Δ_{i+1} 及 Ω_{i+1} 满足条件1)，2)，3). 现若使 $\Omega=\Omega_{r+1}$，它满足引理的条件.

附注. 注意 Ω/Φ 的根塔的各整数 n_i 与 Σ/Φ 的给定塔的整数是相同的.

现在我们可以证明伽罗瓦条件的必要性了：设 $f(x)=0$ 在

特征为 0 的 Φ 上可用根式解，则 $f(x)$ 的分裂域 P/Φ 能被嵌入一个域 Σ 中，它包含 Φ 上的一个根塔，由引理我们可以假设 Σ/Φ 是伽罗瓦扩张．令 n 为出现于 Σ 的一个根塔中的各指数 n_i 的最小公倍数，Δ 是 x^n-1 在 Σ 上的一个分裂域，从而 $\Delta=\Sigma(\zeta)$，这里 ζ 是一个本原 n 次单位根，而且 Δ 是 Φ 上的伽罗瓦扩张，它有一个 Φ 上的根塔．此外，我们可以替 Δ 求得下面形式的根塔：

(11) $\Phi=\Phi_1\subseteq\Phi_2=\Phi_1(\zeta)\subseteq\Phi_3=\Phi_2(\xi_1)\subseteq\cdots\subseteq\Phi_{r+1}(\xi_r)=\Delta$,

这里 $\xi_i^{n_i}\in\Phi_{i+1}$．若 H 是 Δ 在 Φ 上的伽罗瓦群，则子域链(11)给出一个递降的子群链：

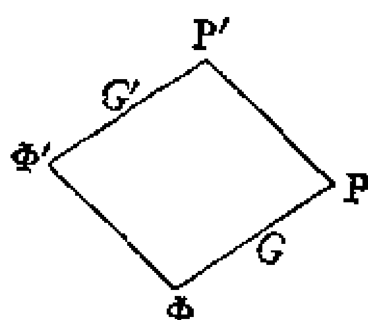
(12) $$H=H_1\supseteq H_2\supsetneq\cdots\supseteq H_{r+2}=1,$$

这里 H_i 是 Δ 在 Φ_i 上的伽罗瓦群．由定理 3，Φ_2 是 Φ_1 上的具有交换伽罗瓦群的伽罗瓦扩张，而且由于 Φ_2 包含了必需的单位根，因此若 $i\geqslant 2$，Φ_{i+1} 是 Φ_i 上的循环扩张．这推得 H_{i+1} 在 $i\geqslant 1$ 时是 H_i 的一个不变子群，商群 H_1/H_2 同构于 Φ_2 在 Φ_1 上的伽罗瓦群，因此是交换的；与此同时，商群 $H_i/H_{i+1}(i\geqslant 2)$ 同构于 Φ_{i+1} 在 Φ_i 上的伽罗瓦群，因此它是循环群．故(12)的群列表明 H 是可解的．现在我们有 $\Delta\supseteq P\supseteq\Phi$，这里 P/Φ 是 $f(x)$ 的分裂域，因此若 K 是对应于 P 的子群，则 K 在 H 中是不变子群且 $H/K\cong G(P/\Phi$ 的伽罗瓦群)．由于 H 是可解的，这表示 G 也是可解的，所以方程 $f(x)=0$ 的伽罗瓦群 G_f 是一个可解群．

为了证明伽罗瓦条件的充分性，我们需要下面的结果，它在单独研究时也很有趣．

定理 6. 设 P/Φ 是 Φ 上的有限维伽罗瓦扩张，P' 是 P 的一个扩张域，这里的 P' 是由 P 及另一子域 $\Phi'\supsetneq\Phi$ 生成的，则 P'/Φ' 是一个有限维伽罗瓦扩张且其伽罗瓦群 G' 同构于 P/Φ 的伽罗瓦群 G 的一个子群(其图解见下页)．

证　我们知道 $P=\Phi(\xi_1,\cdots,\xi_n)$，这里的 ξ_i 是一个可分多项式 $f(x)\in\Phi[x]$ 的根．由于 P' 是 $\Phi'\supseteq\Phi$ 及 P 生成的，我们有 $P'=\Phi'(\xi_1,\cdots,\xi_n)$，因此 P' 是 $f(x)$ 在 Φ' 上的一个分裂域．由于可分性在基域的扩张中是不变的，$f(x)$ 是 Φ' 上的可分多项式，



从而 P′ 是 Φ' 上的伽罗瓦扩张。设 s' 属于 P'/Φ' 的伽罗瓦群 G'，则 s' 在 $\Phi\subseteq\Phi'$ 中是恒等映射而 s' 将集 $R=\{\xi_1,\xi_2,\cdots,\xi_n\}$ 映射到其本身，故 s' 将 $P=\Phi(R)$ 映射到它本身从而 s' 在 P 上的限制是 P 在 Φ 上的伽罗瓦群的一个元 s，映射 $s'\to s$ 是 G' 到 G 内的同态。因为由 $s=1$ 推得 $\xi_i'=\xi_i(1\leqslant i\leqslant n)$，而这又可推得 $s'=1$，故知 $s'\to s$ 是一个同构，从而 G' 同构于 G 的一个子群。

现在我们来证明伽罗瓦条件的充分性：假设 $f(x)=0$ 有一可解伽罗瓦群 G_f，则 $f(x)$ 的分裂域 P/Φ 的伽罗瓦群 G 是可解的。我们仍设 Φ 是特征为 0 的域，使 $n=(G:1)$ 及 $P'=P(\zeta)$，这里 ζ 是一个本原 n 次单位根，则 P′ 由 P 及子域 $\Phi'=\Phi(\zeta)$ 生成，因此由定理 6，P′ 是 Φ' 上的伽罗瓦扩张，而它在 Φ' 上的伽罗瓦群 G' 同构于 G 的一个子群，因此 G' 是可解的，而且有一个合成群列 $G'=G_1'\supset G_2'\supset\cdots\supset G_{s+1}'=1$，其合成因子 G_i'/G_{i+1}' 是素数阶循环群。显然这些阶数是 $n=(G:1)$ 的因子。令

$$\Phi'=\Phi_1'\subset\Phi_2'\subset\cdots\subset\Phi_{s+1}'=P'$$

是对应于 G' 的合成群列的子域链，由于 G_{i+1}' 在 G_i' 中是不变子群，而且 G_i'/G_{i+1}' 是循环群，Φ_{i+1}' 是 Φ_i' 上的伽罗瓦扩张，它具有一个阶为 n 的因子 n_i 的循环伽罗瓦群，由于 $\Phi_i'\supseteq\Phi'=\Phi(\zeta)$，$\Phi_i'$ 包含一个本原 n_i 次单位根，由定理 5 $\Phi_{i+1}'=\Phi_i(\xi_i)$，这里 $\xi_i^{n_i}=\alpha_i\in\Phi_i$，故 $\Phi_1'\subset\Phi_2'\subset\cdots\subset\Phi_{s+1}'=P'$ 是 P′ 在 Φ' 上的一个根塔，由于 $\Phi'=\Phi(\zeta)$，$\zeta^n=1$，$\Phi\subseteq\Phi_1'\subset\Phi_2'\subset\cdots\subset\Phi_{s+1}'=P'$ 是 P′ 在 Φ 上的一个根塔。因为 $P'\supseteq P$，这表明 $f(x)=0$ 在 Φ 上可用根式解。

习　题　20

1. 设 P/Φ 是多项式 x^p-1 在特征为 0 的域 Φ 上的一个分裂域，p 是一个素数，证明：P/Φ 能嵌入一个域 Σ/Φ 之中，后一域有一根塔(10)，使各 n_i 是素数而 $[\Phi_{i+1}:\Phi_i]=n_i$（我们称这样的根塔为正规化根塔（root tower normorlized）(提示：对 p 应用归纳法及§2的习题的第 1 题).

2. 在有理数域 R_0 上求五次及七次单位根的割圆域上的正规化根塔.

3. 证明：若 $f(x)=0$ 有一个在特征为 0 的域上的可解伽罗瓦群，则它的分裂域必能被嵌入一个扩张之中，这个扩张有一个正规化根塔.

4. 设 Φ 是特征 $p\neq 0$ 的域，称方程 $f(x)=0$ ($f(x)\in\Phi[x]$) 可用方程 $x^p-x=\alpha$ 求解，如果它的分裂域 P/Φ 能被嵌入一个域 Σ 之中，Σ 有一个域塔

$$\Phi_1=\Phi\subseteq\Phi_2\subseteq\cdots\subseteq\Phi_{r+1}=\Sigma,$$

这里的 $\Phi_{i+1}=\Phi_i(\xi_i)$，$\xi_i^p-\xi_i=\alpha_i\in\Phi_i$. 证明，若 $f(x)$ 有不同的根，则 $f(x)=0$ 可用方程 $x^p-x=\alpha$ 求解当且仅当它的伽罗瓦群是 p^e 阶的. (提示：利用§2 习题中的第 3,4 题及阶为素数方幂的有限群必是可解群这些事实证明).

4. n 次一般方程　在特征 $\neq 2$ 的域上解二次方程 $x^2-ax+b=0$ 的公式是 $x=(a\pm\sqrt{a^2-4b})/2$，我们常将 a，b 看做未定元；一旦这样处理，我们就有了“二次一般方程”；特殊二次方程是将系数固定后得到的，而在解的公式中作相应的固定就可给出该特殊方程的解. 三次及四次一般方程的根式解法我们也是知道的（见下面习题中的第 3，4 两题）. 我们现在将考虑对于任何 n 的 n 次一般方程的根式解法问题.

设 Φ 为一域而 $\Sigma=\Phi(t_1,t_2,\cdots,t_n)$ 是 Φ 上未定元 t_i 的有理分式域，则方程

(13)　$f(x)=x^n-t_1x^{n-1}+t_2x^{n-2}-\cdots+(-1)^nt_n=0$

称为 Φ 上的 n 次一般方程，我们希望确定这个方程在 Σ 上的伽罗瓦群 G_f. 设 $P=\Sigma(x_1,x_2,\cdots,x_n)$ 是 $f(x)$ 在 Σ 上的一个分裂域，在 $P[x]$ 中

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n),$$

则

(14)　$t_1=\Sigma x_i,\quad t_2=\sum_{i<j}x_ix_j,\cdots,\quad t_n=x_1x_2\cdots x_n;$

因此

(15) $\mathrm{P} = \Sigma(x_1, x_2, \cdots, x_n) = \Phi(t_1, t_2, \cdots, t_n; x_1, \cdots, x_n)$

$= \Phi(x_1, x_2, \cdots, x_n)$.

为了确定 G_f 我们先看一个简单问题：现引进 Φ 上的新未定元 $\xi_1, \xi_2, \cdots, \xi_n$ 以及 ξ_i 的有理分式域 $\bar{\mathrm{P}} = \Phi(\xi_1, \xi_2, \cdots, \xi_n)$. 考虑 $\bar{\mathrm{P}}[x]$ 中的多项式

(16) $$\bar{f}(x) = (x-\xi_1)(x-\xi_2)\cdots(x-\xi_n),$$

我们有

(17) $$\bar{f}(x) = x^n - \tau_1 x^{n-1} + \tau_2 x^{n-2} - \cdots + (-1)^n \tau_n,$$

其中

(18) $$\tau_1 = \Sigma\xi_i, \quad \tau_2 = \sum_{i<j}\xi_i\xi_j, \cdots, \tau_n = \xi_1\xi_2\cdots\xi_n.$$

我们现在考虑 $\bar{\mathrm{P}}/\Phi$ 的子域 $\bar{\Sigma} = \Phi(\tau_1, \tau_2, \cdots, \tau_n)$ 并注意关系 $\bar{\mathrm{P}} = \bar{\Sigma}(\xi_1, \xi_2, \cdots, \xi_n)$ 和 (16) 表明 $\bar{\mathrm{P}}$ 是 $\bar{f}(x)$ 在 $\bar{\Sigma}$ 上的一个分裂域，我们断言方程 $\bar{f}(x) = 0$ 在 $\bar{\Sigma}$ 上的伽罗瓦群 $G_{\bar{f}}$ 是对称群. 为此我们必须证明：若 $\xi_i \to \xi_{i'}$ 是 ξ_i 的任一置换，则存在一个 $\bar{s}_{\bar{f}} \in G_{\bar{f}}$ 使 $\xi_i^{\bar{s}} = \xi_{i'}$. 我们知道有一个 Φ 上的多项式代数 $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ 的使 $\xi_i^{\bar{s}} = \xi_{i'}(1 \leqslant i \leqslant n)$ 的自同构 $\bar{s}$, 我们还知道 $\bar{s}$ 可以扩张为 Φ 上域 $\bar{\mathrm{P}} = \Phi(\xi_1, \xi_2, \cdots, \xi_n)$ 的自同构 $\bar{s}$, 最后 $\bar{s}$ 能扩张到 $\bar{\mathrm{P}}[x]$ 的一个自同构 $\bar{s}$ 使 $x^{\bar{s}} = x$, 因此我们有

$$\bar{f}^{\bar{s}}(x) = (x-\xi_{1'})(x-\xi_{2'})\cdots(x-\xi_{n'}) = \bar{f}(x),$$

由(17)可推得 $\tau_i^{\bar{s}} = \tau_i(1 \leqslant i \leqslant n)$.(这也可利用 τ_i 的表示式(18)看出). 而 $\tau_i^{\bar{s}} = \tau_i$ 可推出 $\bar{\Sigma} = \Phi(\tau_1, \tau_2, \cdots, \tau_n)$ 的元在 $\bar{s}$ 下是固定的. 因此，$\bar{s}$ 是在 $\bar{\mathrm{P}}/\bar{\Sigma}$ 的伽罗瓦群之中，而且其导出映射 $\bar{s}_{\bar{f}}$ 满足 $\xi_i^{\bar{s}} = \xi_{i'}(1 \leqslant i \leqslant n)$. 这就是我们所需要的.

我们将把上面所得到的关于一对域 $\bar{\mathrm{P}}$, $\bar{\Sigma}$ 的结果搬到另一对域 P, Σ 上来，方法是建立 P 到 $\bar{\mathrm{P}}$ 上的一个同构且把 Σ 映射到 $\bar{\Sigma}$ 上. 我们首先考虑 Φ 上的代数同态 η:

$$\Phi[t_1, t_2, \cdots, t_n] \xrightarrow[\eta]{} \Phi[\tau_1, \tau_2, \cdots, \tau_n],$$

它使 $t_i^\eta = \tau_i(1 \leqslant i \leqslant n)$. η 的存在是明显的，因为 t_i 是未定元. 我们断言 η 是一个同构. 为此可注意下面的 Φ 上的同态 ζ:

$$\Phi[\xi_1, \xi_2, \cdots, \xi_n] \xrightarrow[\zeta]{} \Phi[x_1, x_2, \cdots, x_n],$$

因此 $\xi_i^\zeta = x_i$. 这也是明显的,因为 ξ_i 是未定元. 还应注意 $\Phi[\xi_1, \xi_2, \cdots, \xi_n] \supseteq \Phi[\tau_1, \tau_2, \cdots, \tau_n]$, 故 $\eta\zeta$ 被完全确定. 公式(18)与 (14) 表示 $\tau_i^\zeta = t_i$, 因此 $t_i^{\eta\zeta} = \tau_i^\zeta = t_i$, 从而 $g^{\eta\zeta} = g$ 对于 $\Phi[t_1, t_2, \cdots, t_n]$ 中的每个 g 成立,这可推出第一个映射 η 是一个同构, 因为 $g^\eta = 0$ 给出 $g = g^{\eta\zeta} = 0$ 对 $\Phi[t_1, t_2, \cdots, t_n]$ 中的 g 成立。

我们现在要将 η 扩张成 $\Sigma = \Phi(t_1, t_2, \cdots, t_n)$ 到 $\bar{\Sigma} = \Phi(\tau_1, \tau_2, \cdots, \tau_n)$ 上的一个同构 η, 而且它还可扩张成 $\Sigma[x]$ 到 $\bar{\Sigma}[x]$ 上的同构 η 使得 $x^\eta = x$, 因此

$$\begin{aligned} f(x)^\eta &= (x^n - t_1 x^{n-1} + \cdots)^\eta \\ &= x^n - \tau_1 x^{n-1} + \cdots = \bar{f}(x). \end{aligned}$$

另一方面, P 是 $f(x)$ 在 Σ 上的一个分裂域而 $\bar{\mathrm{P}}$ 是 $\bar{f}(x)$ 在 $\bar{\Sigma}$ 上的一个分裂域,分裂域的一般唯一性定理(定理 1.7)为我们提供了一个 P 到 $\bar{\mathrm{P}}$ 上的同构 η, 这个同构在 Σ 上与已知的 η 重合, 由这样的一个同构的存在性立即可见: P/Σ 的伽罗瓦群 G 同构于 $\bar{\mathrm{P}}/\bar{\Sigma}$ 的伽罗瓦群 $\bar{G}$. 事实上, 映射 $s \to \eta^{-1}s\eta$ 显然是 G 到 $\bar{G}$ 上的一个同构. 由 $G_{\bar{f}} = S_n$ 这一事实可推出 $f(x) = 0$ 在 Σ 上的伽罗瓦群 G_f 是 S_n. 还可以清楚看到 $f(x)$ 的根是不相同的, 定理 2 表示 $f(x)$ 在 $\Sigma[x]$ 中是不可约的. 我们所得到的结果可叙述如下:

定理 7. n 次一般方程 (13) 在 $\Sigma = \Phi(t_1, t_2, \cdots, t_n)$ 中不可约而且有不同的根, $f(x) = 0$ 的伽罗瓦群是对称群 S_n.

由于 S_n 在 $n > 4$ 时不是可解群,故有

阿贝尔-努芬尼定理. n 次一般方程当 $n > 4$ 时不能用根式解 (域的特征为 0).

习　题　21

1. 利用每个有限群都同构于 S_n 的一个子群这一事实,构造一个域 P 使它在一适当的域 Φ 上的伽罗瓦群同构于一已知的有限群 G(对于已知的 Φ 及 G 构造 P 是一个尚未解决的问题,事实上,甚至对于 Φ 是有理数域的情况这还是一个尚未解决的古典问题).

2. 利用伽罗瓦理论证明：若 $r(x_1, x_2, \cdots, x_n) \in \Phi(x_1, x_2, \cdots, x_n)$，这里的 $\Phi(x_1, x_2, \cdots, x_n)$ 是域 Φ 上含未定元 x_i 的有理分式域，而 r 是通常意义下的对称式，即 $r(x_{1'}, x_{2'}, \cdots, x_{n'}) = r(x_1, x_2, \cdots, x_n)$ 对于各 x 的每个置换 $x_i \to x_{i'}$ 都成立的式子，则 r 是一个系数在 Φ 中的、含各初等对称多项式 $t_1 = \Sigma x_i$，$t_2 = \sum_{i<j} x_i x_j$，$\cdots$，$t_n = x_1 x_2 \cdots x_n$ 的有理式(将本结果与卷 1 的中译本 p.102 的对称多项式基本定理比较)。

3. 假设 Φ 的特征不是 2 或 3，今考察三次一般方程

$$x^3 - t_1 x^2 + t_2 x - t_3 = (x - x_1)(x - x_2)(x - x_3),$$

这里 t_i 是未定元，x_i 在 $\Sigma = \Phi(t_1, t_2, t_3)$ 上的一个分裂域 P 之中. 今用

$$y_i = x_i - \frac{1}{3}(x_1 + x_2 + x_3) = x_i - \frac{1}{3} t_1$$

代替 x_i，则所给方程变成 $y^3 + py + q = 0$，它的根 y_1, y_2, y_3 满足 $y_1 + y_2 + y_3 = 0$，判别式公式(6)此时变成，$\delta = -4p^3 - 27q^2$，P 在 $\Sigma(\sqrt{\delta})$ 上的群是交代群 A_3，它是 3 阶循环群. 设 ξ 是一个本原三次单位根$\left(例如 \xi = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}\right)$ 并令

$$z_1 = y_1 + \xi^{-1} y_2 + \xi^{-2} y_3 = y_1 + \xi^2 y_2 + \xi y_3,\ z_2 = y_1 + \xi^{-2} y_2 + \xi^{-4} y_3$$
$$= y_1 + \xi y_2 + \xi^2 y_3, z_3 = y_1 + y_2 + y_3 = 0.$$

验证：如果 $\xi = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$，则 $z_1^3 = -\frac{27}{2} q - \frac{3}{2}\sqrt{-3}\sqrt{\delta}$，$z_2^3 = -\frac{27}{2} q + \frac{3}{2}\sqrt{-3}\sqrt{\delta}$，$z_1 z_2 = -3p$. 因此

$$z_1 = \sqrt[3]{-\frac{27}{2} q - \frac{3}{2}\sqrt{-3\delta}}, \tag{19}$$

$$z_2 = \sqrt[3]{-\frac{27}{2} q + \frac{3}{2}\sqrt{-3\delta}}.$$

这里 $\sqrt{-3\delta}$ 的确定在两个公式中应是相同的，至于 $\sqrt[3]{\ }$ 的取法须能满足 $z_1 z_2 = -3p$. 解方程组 $z_1 = y_1 + \xi^2 y_2 + \xi y_3, z_2 = y_1 + \xi y_2 + \xi^2 y_3, z_3 = y_1 + y_2 + y_3$ 求 y_1, y_2, y_3 就能得到方程 $y^3 + py + q = 0$ 的卡达诺 (Cardano) 求解公式.

4. 设特征不是 2 或 3，考虑四次一般方程

$$x^4 - t_1 x^3 + t_2 x^2 - t_3 x + t_4 = (x - x_1)(x - x_2)(x - x_3)(x - x_4),$$

用 $y_i = x_i - \frac{1}{4} t_1$ 代替 x_i 后得方程 $f(y) = y^4 + py^2 + qy + r = 0$，它的根是 y_1, y_2, y_3, y_4. 证明 $f(y) = 0$ 的三次预解式是

$$g(z) = z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0$$

(参看 §1 习题). 证明 $\mathrm{P} = \Phi(x_1, x_2, x_3, x_4) = \Phi(y_1, y_2, y_3, y_4)$ 在 $\Phi(z_1, z_2, z_3)$ (z_i 是 $g(z) = 0$ 的根)上的伽罗瓦群是四元群. 找出利用 z_1, z_2, z_3 及 $\Phi(z_1, z_2, z_3)$ 的元的平方根求 y_1, y_2, y_3, y_4 的公式.

5. 考察一般方程(13)在 $\Sigma=\Phi(t_1,\cdots,t_n)$ (t_i 是未定元) 上的一个分裂域 P，并设 $x_1,x_2,\cdots,x_n$ 是它的根. 假设 Φ 包含 n 个不同的元 $c_1,c_2,\cdots,c_n$，证明

$$\theta=c_1x_1+c_2x_2+\cdots+c_nx_n$$

是 P/Σ 的一个本原元.

5. 以对称群作为伽罗瓦群的有理系数方程 阿贝尔-努芬尼定理表明次数 $\geqslant 5$ 且以未定元为系数的方程不能用根式解，但另一方面，对于某些域 Φ(例如实数域或复数域)，每个系数在 Φ 中的方程却是能够用根式解的. 我们现在将要指出：存在不能用根式解的有理系数方程. 为此我们将证明存在任意素数 p 次的有理系数方程，它以对称群 S_p 作为伽罗瓦群. 我们首先证明置换群的下列结果.

引理. 若 G 是 p 个元上的一个置换群 (这里 p 是一个素数) 而且 G 包含一个阶为 p 的元及一个对换，则 $G=S_p$.

证. 我们知道任一置换均可写成不相交的循环之积(卷 1 的中译本 p.36)；此外，一个循环的阶等于它所包含的文字的个数. 由此推出：若 $\sigma\in G$ 有阶 p，则 σ 是一个包含所有这些文字 1，2，…，p 的循环. 适当重排元 1，2，…的次序，我们可假设 G 包含对换(12)；由于 p 元循环 σ 的一个适当方幂有形式(12…)，必要时还可通过重排元素 12，…，p 的次序，使我们可以假设 G 包含 (12) 及 $\sigma=(123\cdots p)$；我们还知道，若 τ 是 S_p (或 S_n) 的任一元，则 $\tau^{-1}(ij)\tau=(i^\tau j^\tau)$，这里的 i^τ，j^τ 分别是 i，j 在 τ 下的象. 这表示 $\sigma^{-1}(12)\sigma=(23)$，$\sigma^{-2}(12)\sigma^2=(34)$，$\cdots$，$(p-1,p)$ 及 $(p1)$ 都包含于 G 之中，由于

$$\begin{aligned}(13)&=(12)(23)(12)\\(14)&=(13)(34)(13)\\&\vdots\\(1p)&=(1p-1)(p-1p)(1p-1)\end{aligned}$$

所有这些元都包含于 G 之中；由于当 1，i，j 不相同时 $(ij)=(1i)(1j)(1i)$，这又表示每个对换都包含于 G 之中. 由于 S_p 的每个元都可表成对换的乘积，故有 $G=S_p$.

我们现在证明

定理 8. 令 $f(x)$ 是一个在有理数域上不可约的素数次有理系数多项式，假若 $f(x)=0$ 在复数域 C 中恰有两个非实根，则 $f(x)=0$ 在有理数域上的群 G_f 是对称群。

证 代数基本定理断言：在 $C[x]$ 内

$$f(x)=(x-\rho_1)(x-\rho_2)\cdots(x-\rho_p),$$

因此 C 的子域 $P=R_0(\rho_1,\rho_2,\cdots,\rho_p)$（$R_0$ 是有理数域）是 $f(x)$ 在 R_0 上的一个分裂域。由于 $P\supseteq R_0(\rho_1)$ 及 $[R_0(\rho_1):R_0]=\deg f(x)=p$，$[P:R_0]$ 能被 p 整除，因此 p 是 $(G:1)$ 的一个因子，这里的 G 是 P 在 R_0 上的伽罗瓦群。由西罗定理知 G 包含一个阶为 p 的元。现考虑 C 在实数域上的自同构

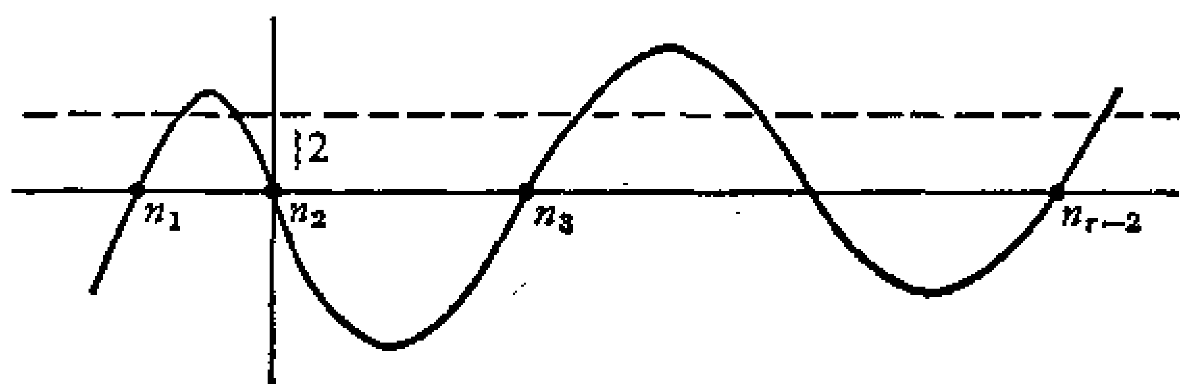
$$a=\alpha+\beta\sqrt{-1}\to\alpha-\beta\sqrt{-1}=\bar{a}$$

（α, β 是实数），这个自同构将 $f(x)$ 映射到它本身内去，这是因为 $f(x)$ 的系数是实数，而且它还把属于 C 的 $f(x)$ 的根集$\{\rho_1,\rho_2,\cdots,\rho_p\}$ 映射到它本身内去。设 ρ_1, ρ_2 是 $f(x)$ 的非实数根，则 $a\to\bar{a}$ 将 ρ_1 与 ρ_2 互换而使所有 $\rho_i(i>2)$ 不变，因此 C 的自同构 $a\to\bar{a}$ 对于这个根集的限制是 G_f 的一个元，它是一个对换。故 G_f 包含一个阶为 p 的元及一个对换，由引理知 $G_f=S_p$。

我们如下构造满足定理条件的多项式[1]：设 m 是一个正整数，$n_1<n_2<\cdots<n_{r-2}$ 是 $r-2$ 个偶数，这里 r 是 >3 的奇数。看多项式

(20) $\quad g(x)=(x^2+m)(x-n_1)(n-n_2)\cdots(x-n_{r-2})$。

$g(x)$ 的实根是 $n_1,n_2,\cdots,n_{r-2}$，而 $y=g(x)$ 的图象是



1) 这个构造法是 R. 布劳尔（Brauer）给出的。——著者注。

这个多项式有 $(r-3)/2$ 个相对极大值，而且对于任何奇数 k 都有 $|g(k)|>2$，所以这些相对极大值都 >2. 由此推出 $f(x)=g(x)-2$ 在 n_1 与 n_{r-2} 之间有 $(r-3)/2$ 个正相对极大值，进而推得 $f(x)$ 有 $r-3$ 个实根在区间 (n_1, n_{r-2}) 内. 由于 $f(n_{r-2})=-2$ 及 $f(\infty)=\infty$，所以还有一实根 $>n_{r-2}$. 这就给出了 $f(x)$ 的 $r-2$ 个实根. 使 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 $f(x)$ 的复数根，则 $f(x)=\Pi(x-\alpha_i)=(x^2+m)(x-n_1)\cdots(x-n_{r-2})-2$，使两端的 x^{r-1} 项与 x^{r-2} 项的系数相等可得

$$(21)\qquad \sum_1^r \alpha_i=\sum_1^{r-2} n_k,\quad \sum_{i<j}\alpha_i\alpha_j=\sum_{k<l} n_k n_l+m.$$

因此

$$(22)\qquad \Sigma\alpha_i^2=(\Sigma\alpha_i)^2-2\sum_{i<j}\alpha_i\alpha_j=\Sigma n_k^2-2m.$$

当 m 选择得充分大时，由(22)可知我们能使 $\Sigma\alpha_i^2<0$，而这说明不是所有的 α_i 是实数，今设 α_1 是一个非实数根，则 $\bar{\alpha}_1\neq\alpha_1$ 是另一个这样的根，因此我们至少有两个非实数根. 由于在任何场合我们都有 $r-2$ 个实根，可知 $f(x)$ 恰有 $r-2$ 个实根. 将它写成 $f(x)=x^r+a_1x^{r-1}+\cdots+a_r$，显然各 a_i 是偶数. 此外，由于 $g(x)$ 的常数项能被 4 整除，所以 $f(x)=g(x)-2$ 的常数项就不能被 4 整除. 将艾森斯坦 (Eisenstein) 判定法应用到素数 $q=2$ 的场合就可知 $f(x)$ 在有理数域上是不可约的. 由此可知对于每个素数 $p=r\geqslant 5$，我们是能够满足定理条件的. 还易见这也对 $p=2, 3$ 时成立. 因此条件对每个素数均成立，这就证明了确实存在任意素数 p 次的、以对称群 S_p 为其伽罗瓦群的有理系数方程.

习　题　22

1. 设 $f(x)\in\Phi[x]$ 在一个分裂域 P/Φ 中有不同的根 $\rho_1, \rho_2, \cdots, \rho_n$，$G_f\subseteq S_n$ 是方程 $f(x)=0$[1] 的伽罗瓦群，$y_1, y_2, \cdots, y_n$ 是未定元并使

1) 原书误排为"方程 f". ——译者注.

$$F(x)=\prod_{t\in S_n}(x-(\rho_{1t}y_1+\rho_{2t}y_2+\cdots+\rho_{nt}y_n))$$

$$=\prod_{t\in S_n}(x-(\rho_1 y_{1t}+\rho_2 y_{2t}+\cdots+\rho_{nt})),$$

证明 $F(x)\in\Phi[y_1,y_2,\cdots,y_n,x]$. 设 $F(x)=F_1(x)F_2(x)\cdots F_r(x)$ 是 $F(x)$ 在 $\Phi(y_1,y_2,\cdots,y_n)[x]$ 中的分解成首项系数为1的不可约因子的分解式. 证明: 若 $x-\sum_i\rho_{it}y_i$ 是 $F_1(x)$ 的一个因子,则

$$F_1(x)=\prod_{t\in G_f}(x-\sum_i\rho_{it_i})$$

由此证明 $\deg F_i(x)=(G_f:1)$.

2.符号如同题1,此外,设 $\Phi=R_0$ (R_0 是有理数域), 又 $f(x)$ 是首项系数为1的整系数多项式. 假设 p 是一个素数, 它能使多项式 $\bar f(x)$ ($\bar f(x)$ 是将 $f(x)$ 的系数用它们的模 p 的剩余数代入得到的) 在一个分裂域 $\bar{\mathrm{P}}/I_p$ 中有不同的根. 证明: 在 $\bar{\mathrm{P}}[x,y_1,\cdots,y_n]$ 中 $\bar F(x)=\prod_{t\in S_n}(x-\bar\rho_i y_{it})$,这里 $\bar\rho_1,\bar\rho_2,\cdots,\bar\rho_n$ 是 $\bar f(x)$ 在 $\bar{\mathrm{P}}$ 中的根. 利用此结果及题1 证明: 若将 $\bar\rho_i$ 适当排列,则 $G_{\bar f}$ 是 G_f 的一个子群.

3.证明: 若 S_n 的任一可迁子群包含一个 $n-1$ 元循环及一个对换,那末它必和 S_n 重合.

4.证明方程

$$x^6+22x^5-9x^4+12x^3-37x^2-29x-15^{1)}=0$$

在 R_0 上有群 S_6(提示: 利用第2题,使素数 $p=2,3,5$.)

1) 原书此处无"=0"字样. ——译者注.

第三章

阿贝尔扩张

本章将研究阿贝尔扩张域的几种类型．首先讨论有理数域上的割圆域，并确定它们的维数及伽罗瓦群；其次讨论库默尔(Kummer)扩张，它是由添加纯方程 $x^m = \alpha$ 的有限个根到一个含 m 个不同的 m 次单位根的域得到的；最后研究阿贝尔 p 扩张，它是特征 $p \neq 0$ 的域的 p^l 维阿贝尔扩张．有限交换群的特征标理论是研究库默尔扩张和阿贝尔 p 扩张的基本工具．此外，研究阿贝尔 p 扩张还要以维特(Witt)向量环为基础，它可由特征 $p \neq 0$ 的域上任意交换代数 $\mathfrak{A}$ 构造出来，对于任何这样的 $\mathfrak{A}$ 和整数 $m = 1, 2, \cdots$，就有一个特征为 p^m 的维特向量环 $\mathfrak{W}_m(\mathfrak{A})$．在赋值论中，我们常取 $m \to \infty$ 时的极限并考虑无限维特向量环 $\mathfrak{W}(\mathfrak{A})$，这将在第五章讨论．本章的若干结果在第六章形式实域理论的应用中需要．

1. 有理数域上的割圆域 我们曾定义域 Φ 上 m 次割圆域是多项式 $x^m - 1$ 在 Φ 上的分裂域(§ 2.2)，而且证明了：当 Φ 的特征不是 m 的因子时，割圆域的伽罗瓦群同构于环 $I/(m)$ 中单位所成群 $U(m)$ 的子群(定理 2.3)．今设基域 $\Phi = R_0$ 为有理数域，$\mathrm{P}^{(m)}$ 表示 R_0 上 m 次单位根所成的割圆域．令 $Z(m)$ 是 m 次单位根的乘法群．我们知道 $Z(m)$ 是循环群，它的生成元叫作 m 次本原单位根，而且 $\mathrm{P}^{(m)} = R_0(\zeta)$，其中 ζ 是任一 m 次本原单位根；所以维数 $[\mathrm{P}^{(m)}:R_0]$ 是 ζ 在 R_0 上的最小多项式的次数．如果 ζ 是 m 次本原单位根，则其余 m 次本原单位根形如 ζ^k，这里 $(k, m) = 1$．所以 m 次本原单位根有 $\varphi(m)$ 个，即不超过 m 而与 m 互素的正整数的个数，也就是群 $U(m)$ 的阶．

令

$$\lambda_m(x)=\prod_{\zeta\text{本原}}(x-\zeta), \tag{1}$$

这是一个系数在 $P^{(m)}$ 中的 $\varphi(m)$ 次多项式。如果 s 属于 R_0 上 $P^{(m)}$ 的伽罗瓦群 G，显然 s 将 m 次本原单位根的集合映到其自身内。因此，对于每一 $s\in G$，$\lambda_m^s(x)=\lambda_m(x)$。又因为 $P^{(m)}$ 是 R_0 上的伽罗瓦扩张，可见 $\lambda_m(x)\in R_0[x]$，即 $\lambda_m(x)$ 是有理系数多项式。我们还可以用更为初等的方法来考察它，进而得到一种计算 $\lambda_m(x)$ 的归纳步骤。因为任何 m 次单位根的阶都是 m 的因子，而当 $d|m$ 时，每一 d 次单位根都是 m 次单位根，于是有公式：

$$x^m-1=\prod_{\substack{d|m\\1\leqslant d\leqslant m}}\lambda_d(x). \tag{2}$$

显然 $\lambda_1(x)=x-1$，现假设对一切满足 $1\leqslant d<m$ 的 d，有 $\lambda_d(x)\in R_0[x]$，那末公式 (2) 给出

$$\lambda_m(x)=(x^m-1)\Big/\prod_{d|m}\lambda_d(x). \tag{3}$$

这表明 $\lambda_m(x)\in R_0[x]$，而且给出了计算 $\lambda_m(x)$ 的实际方法。例如，我们有 $\lambda_1(x)=x-1$，

$$\begin{aligned}
\lambda_2(x)&=(x^2-1)/\lambda_1(x)=x+1,\\
\lambda_3(x)&=(x^3-1)/\lambda_1(x)=x^2+x+1,\\
\lambda_4(x)&=(x^4-1)/\lambda_1(x)\lambda_2(x)=x^2+1,\\
\lambda_6(x)&=(x^6-1)/\lambda_1(x)\lambda_2(x)\lambda_3(x)\\
&=x^2-x+1,
\end{aligned}$$

而且

$$\begin{aligned}
\lambda_{12}(x)&=(x^{12}-1)/\lambda_1(x)\lambda_2(x)\lambda_3(x)\lambda_4(x)\lambda_6(x)\\
&=x^4-x^2+1.
\end{aligned}$$

如果 p 是素数，我们有

$$\begin{aligned}
\lambda_p(x)&=(x^p-1)/(x-1)\\
&=x^{p-1}+x^{p-2}+\cdots+1.
\end{aligned} \tag{4}$$

由艾森斯坦准则容易看出 $\lambda_p(x)$ 是 $R_0[x]$ 的不可约多项式(卷 1 的中译本 p.118 习题50的第 2 题)现证明下面的一般结果：

定理 1. $\lambda_m(x)$ 在有理数域上是不可约的.

证 首先 $\lambda_m(x)$ 是整系数多项式. 假如 $d<m$ 时,此结论对每一 $\lambda_d(x)$ 是成立的,令 $p(x)=\prod_{\substack{d|m\\1\leqslant d<m}}\lambda_d(x)$, 用带余除法得到 $x^m-1=p(x)q(x)+r(x)$, 此处 $q(x), r(x)\in I[x]$, $\deg r(x)<\deg p(x)$. 另一方面有 $x^m-1=p(x)\lambda_m(x)$, 由商及余式的唯一性可得 $\lambda_m(x)=q(x)$ 有整数系数. 现设 $\lambda_m(x)=h(x)k(x)$, 此处 $h(x)\in R_0[x]$ 是不可约的, $\deg h(x)\geqslant 1$. 由高斯引理(卷1的中译本 p.116) 可假设 $h(x)$ 与 $k(x)$ 是首项系数为1的整系数多项式. 令 p 是素数且 $p\nmid m$, ζ 是 $h(x)$ 的根. 我们将证明 ζ^p 是 $h(x)$ 的根. 因为 $(p, m)=1$, ζ^p 是 m 次本原单位根. 如果 ζ^p 不是 $h(x)$ 的根,则 ζ^p 是 $k(x)$ 的根,于是 ζ 是 $k(x^p)$ 的根. 由于 $h(x)$ 在 $R_0[x]$ 中不可约,且有 ζ 为根,故 $h(x)\mid k(x^p)$. 于是 $k(x^p)=h(x)l(x)$, $l(x)$ 是首项系数为1的整系数多项式. 我们还有

$$x^m-1=\lambda_m(x)p(x)=h(x)k(x)p(x),$$

这些都是首项系数为1的整系数多项式. 通过取同余模 p 或同样地化为多项式环 $I_p[x]$ 中的关系,得到

$$x^m-\bar{1}=\bar{h}(x)\bar{k}(x)\bar{p}(x). \tag{5}$$

一般地,如果 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n\in I[x]$, 那末

$$\bar{f}(x)=\bar{a}_0x^n+\bar{a}_1x^{n-1}+\cdots+\bar{a}_n,\quad \bar{a}_i=a_i+(p)\in I_p.$$

类似地有 $\bar{k}(x^p)=\bar{h}(x)\bar{l}(x)$. 另外,因为对每个整数 a 都有 $\bar{a}^p=\bar{a}$, 所以对任何多项式 $f(x)$ 都有

$$\begin{aligned}\bar{f}(x)^p&=(\bar{a}_0x^n+\cdots+\bar{a}_n)^p=\bar{a}_0^px^{pn}+\cdots+\bar{a}_n^p\\&=\bar{a}_0x^{pn}+\cdots+\bar{a}_n=\bar{f}(x^p).\end{aligned}$$

因此 $\bar{k}(x)^p=\bar{k}(x^p)=\bar{h}(x)\bar{l}(x)$, 由此推出 $(\bar{h}(x), \bar{k}(x))\neq 1$, 则 (5) 表明 $x^m-\bar{1}$ 在 I_p 上的分裂域中有重根. 因为 $p\nmid m$, 这是不可能的. 这就证明了对于每一个满足 $p\nmid m$ 的素数 p, ζ^p 是 $h(x)$ 的根. 重复这一步骤表明,对于每一与 m 互素的整数 r, ζ^r 是 $h(x)$ 的根. 因为任一 m 次本原单位根都形如 $\zeta^r((r, m)=1)$, 可见每一 m 次本原单位根都是 $h(x)$ 的根, 所以 $h(x)=\lambda_m(x)$, $\lambda_m(x)$

在 $R_0[x]$ 中是不可约的.

至此我们已看到，$\lambda_m(x)$ 是任一 m 次本原单位根在 R_0 上的最小多项式. 因为 $P^{(m)} = R_0(\zeta)$，ζ 是本原的，我们已经得到公式

$$[P^{(m)}:R_0] = \varphi(m). \tag{6}$$

由此推出：对 $P^{(m)}/R_0$ 的伽罗瓦群 G 有 $(G:1) = \varphi(m)$. 因为 $(U(m):1) = \varphi(m)$，且 G 同构于 $U(m)$ 的子群. 这就证明了

定理 2. 令 $P^{(m)}$ 是有理数域 R_0 上的 m 阶割圆域，则 $P^{(m)}/R_0$ 的伽罗瓦群同构于环 $I/(m)$ 中单位所成的乘群 $U(m)$.

现在来决定伽罗瓦群 G(亦即 $U(m)$) 的构造. 易见，如果 $m = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$，$p_i$ 是不同素数，则 $U(m)$ 同构于 $U(p_i^{e_i})$ 的直积，因此只须考虑素数幂 $m = p^e$ 的情形就够了，此时 $U(p^e)$ 是 $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ 阶交换群. 我们先证

定理 3. 若 p 是奇素数，则 $I/(p^e)$ 的单位所成乘法群 $U(p^e)$ 是循环群.

证　因为这个群的阶是 $p^{e-1}(p-1)$，则 $U(p^e)$ 是子群 H 和子群 K 的直积，其中 H 是由满足 $x^{p^{e-1}} = 1$ 的元组成的 p^{e-1} 阶子群，K 是由满足 $x^{p-1} = 1$ 的元组成的 $p-1$ 阶子群. 根据阶互素的循环群的直积仍是循环群，故只须证明 H 和 K 都是循环群就够了. 若 $e = 1$，则 $U(p) = K$ 是域 $I/(p)$ 的乘法群，并且是循环群，因此能选择整数 a，使 $a + (p), a^2 + (p), \cdots, a^{p-1} + (p)$ 在 $I/(p)$ 中是不同的. 令 $b = a^{p^{e-1}}$，由于 $(a,p) = 1$，$(b, p^e) = 1$，且 $b + (p^e)$，$a + (p^e) \in U(p^e)$. 又因为 $b^{p-1} = (a^{p^{e-1}})^{p-1} = a^{\varphi(p^e)} \equiv 1 \pmod{p^e}$，于是 $b + (p^e) \in K$. 因为 $b = a^{p^{e-1}} \equiv a \pmod{p}$，所以 $b + (p), b^2 + (p), \cdots, b^{p-1} + (p)$ 是不同的，故 $b + (p^e)$，$b^2 + (p^e), \cdots, b^{p-1} + (p^e)$ 也是不同的，因此 $b + (p^e)$ 的阶恰是 $p-1$. 由于 $(K:1) = p-1$，所以 K 是以 $b + (p^e)$ 为生成元的循环群. 剩下要证明 H 是循环群，不妨假设 $e \geq 2$，否则 $H = (1)$，其结果是显然的. 设 $e \geq 2$，可以断定 H 是 $k \geq 1$ 个 $p^{e_i}(e_i \geq 1)$ 阶循环群的直积. 从而方程 $x^p = 1(x \in H)$ 有 p^k 个解. 下面只须证明满足 $n^p \equiv 1 \pmod{p^e}$ 的整数 $n(0 < n < p^e)$

不超过 p 个就够了. 今设 n 满足这些条件,则由于 $n^p \equiv n(\bmod p)$,故有 $n \equiv 1(\bmod p)$.因此,如果 $n \neq 1$,则可写成 $n = 1 + yp^f + zp^{f+1}$,此处 $1 \leqslant f \leqslant e-1$,$0 < y < p$,$z$ 是一个非负整数,所以

$$n^p = 1 + \binom{p}{1}(y + zp)p^f + \binom{p}{2}(y + zp)^2 p^{2f} + \cdots$$

$$+ (y + zp)^p p^{pf} \equiv 1 + yp^{f+1}(\bmod p^{f+2}).$$

如果 $n^p \equiv 1(\bmod p^e)$ 而且 $f < e - 1$,这就给出

$$yp^{f+1} \equiv 0(\bmod p^{f+2}),$$

于是 $y \equiv 0(\bmod p)$,这与 $0 < y < p$ 矛盾. 所以我们知道如果 n 满足 $1 < n < p^e$ 及 $n^p \equiv 1(\bmod p^e)$,则 $n = 1 + yp^{e-1}$, $0 < y < p$. 所以包含 1 在内的全部解至多有 p 个. 证毕.

下面考虑素数 2 的情形.

定理 4. $U(2)$ 和 $U(4)$ 是循环的,当 $e \geqslant 3$ 时,$U(2^e)$ 是一个 2 阶循环群和一个 2^{e-2} 阶循环群的直积.

证 $U(2^e)$ 的阶是 $\varphi(2^e) = 2^{e-1}$. 如果 $e = 1$,则

$$(U(2):1) = 1.$$

如果 $e = 2$,则 $U(2^e) = U(4)$ 仅有两个元,所以是循环的. 假设 $e \geqslant 3$,我们首先证明有四个不同元 $x \in U(2^e)$ 满足 $x^2 = 1$. 这就可推出 $U(2^e)$ 是至少两个 $\neq 1$ 的不同循环群的直积. 令 $a_1 = 1$, $a_2 = -1$, $a_3 = 1 + 2^{e-1}$, $a_4 = -1 + 2^{e-1}$, $x_i = a_i + (2^e)$.则 x_i 是不同的,且满足 $x_i^2 = 1$,这就证明了我们的论断. 又由于 $U(2^e)$ 是至少两个 $\neq 1$ 的循环群的直积,而 $U(2^e)$ 的阶为 2^{e-1},可见若 $x \in U(2^e)$,则 $x^{2^{e-2}} = 1$. 或者说:若 a 是奇整数,则

$$a^{2^{e-2}} \equiv 1(\bmod 2^e).$$

因此只要找到满足 $x^{2^{e-3}} \neq 1$ 的 x,定理就证实了. 因为这就得到了一个 2^{e-2} 阶循环子群,而此仅在 $U(2^e)$ 是一个 2^{e-2} 阶循环群和一个 2 阶循环群的直积时才能成立. 为此,可取 $x = 5 + (2^e)$. 先注意到:若 $e = 3$,则 $5^{2^{e-3}} = 5 \neq 1(\bmod 2^e)$,但

$$5^{2^{e-2}} \equiv 1(\bmod 2^{e-1}),$$

令 $f \geqslant 3$，且 $k(f)$ 是使 $5^{2^{f-3}} \equiv 1 (\bmod 2^k)$ 成立的最大整数 k，则 $k(3) = 2$，对任何 $f \geqslant 3$，有 $5^{2^{f-3}} = 1 + y2^{k(f)}$，其中 y 是奇数。因此得

$$5^{2^{(f+1)-3}} = (5^{2^{f-3}})^2 = 1 + y2^{k(f)+1} + y^2 2^{2k(f)}.$$

这首先表明，当 $f \geqslant 3$ 时，$k(f+1) \geqslant k(f)$，故 $k(f) \geqslant 2$. 其次，关系式表明 $5^{2^{(f+1)-3}} = 1 + z2^{k(f)+1}$，其中，$z = y + 2^{k(f)-1}y^2$ 是奇数，因此有 $k(f+1) = k(f) + 1$，再利用 $k(3) = 2$ 推出：对一切 $f \geqslant 3$ 有 $k(f) = f - 1$，故当 $e \geqslant 3$ 时 $5^{2^{e-3}} \not\equiv 1 (\bmod 2^e)$. 这就是我们要证的. 证毕.

定理 2，3 和 4 描述了有理数域上 p^e 次单位根域的伽罗瓦群，概括如下.

定理 5. 设 $m = p^e$，p 是素数，$P^{(m)}$ 是有理数域 R_0 上 m 次单位根的域. 则 $P^{(m)}/R_0$ 的伽罗瓦群 G 是循环群(除 $p = 2$，$e \geqslant 3$ 外). 在这一例外情形下，G 是 2 阶与 2^{e-2} 阶循环群的直积.

习　题　23

1. 用默比乌斯反演公式(卷1，中译本 p. 112，习题 47 的第 5 题)证明.

$$\lambda_m(x) = \prod_{d \mid m} (x^d - 1)^{\mu\left(\frac{m}{d}\right)}.$$

2. 令 p 是素数，$P^{(p)}$ 是有理数域 R_0 上 p 次单位根的割圆域. 令 $g + (p)$ 是循环群 $U(p)$ 的生成元，s 是 $P^{(p)}/R_0$ 的使 $\zeta^s = \zeta^g$ 的自同构，ζ 是取定的 p 次本原单位根. 证明 $(\zeta, \zeta^s, \zeta^{s^2}, \cdots, \zeta^{s^{p-2}})$ 形成 $P^{(p)}/R_0$ 的一个基(正规基). 假设 $p - 1 = ef$，e，f 是正整数，E/R_0 是 $P^{(p)}/R_0$ 的 e 维子域. 证明：如果 $t = s^e$，$\eta = \zeta + \zeta^t + \zeta^{t^2} + \cdots + \zeta^{t^{f-1}}$，那末 $(\eta, \eta^s, \cdots, \eta^{s^{e-1}})$ 是 E/R_0 的一个基. 证明：关于这个基的乘法表有整系数.

3. 令 P 是 R_0 上 17 次单位根的域，作子域 $R_i (i = 1, 2, 3)$ 使 $R_0 \subset R_1 \subset R_2 \subset R_3 \subset R_4 = P$，$[R_i : R_{i-1}] = 2$. 在 R_i 中求一个元素 ω_i 使 $R_i = R_{i-1}(\omega_i)$，$\omega_i^2 \in R_{i-1}$，$1 \leqslant i \leqslant 4$.

4. (O. 妥特 (O. Todd)) 令 P 是 R_0 上 p 次单位根的域，p 是形如 $4m + 3$ 的素数，证明 P 是一个二次子域与一个奇数维的子域的张量积，并证明这个二次子域不是实域(如果将 P 看作复数域的子域).

5. 令 $E^{(m)}$ 是 $\Phi_0 = I_p$ 上 m 次割圆域，记 $m = m'p^e$，$(m', p) = 1$，证明 $[E^{(m)} : \Phi_0]$ 是群 $U(m')$ 中元素 $p + (m')$ 的阶.

2. 有限交换群的特征标 本章余下的部分要研究两类阿贝尔扩张域：库默尔扩张与特征为 p 的域上 p^e 维阿贝尔扩张．它们都要以有限交换群的特征标理论为基础．所以我们先加以讨论．

令 A 和 B 是两个交换群(运算用乘法记)，χ 和 ψ 是 A 到 B 内的同态，定义它们的乘积 $\chi\psi$ 为 $a^{\chi\psi}=a^{\chi}a^{\psi}$，验算可知 $\chi\psi$ 也是一个同态，而且 A 到 B 内的一切同态集 $\mathrm{Hom}(A, B)$ 在乘积 $\chi\psi$ 下是一个交换群(参考卷1，中译本 p.74)．我们特别感兴趣的情况是：A 有限，$B=Z$ 是有限循环群，Z 的阶被 A 的所有元的阶整除．我们把 A 的元的最大阶数叫作 A 的**指数**．我们知道群的每个元的阶整除其指数(卷 2，中译本 p.61，习题中的第 1 题)．因此，对 Z 所加的条件等价于 Z 的阶被 A 的指数整除．

我们希望由 A 的特殊分解式 $A=A_1\times A_2\times\cdots\times A_r$ 来决定 $\mathrm{Hom}(A, Z)$，此处 A_i 是循环子群．设 $A=A_1A_2\cdots A_r$，$A_i\cap A_1\cdots A_{i-1}A_{i+1}\cdots A_r=1$．令 $n_i=(A_i:1)$，C_i 是 Z 中满足 $z^{n_i}=1$ 的元 z 作成的子群．由于 n_i 是 Z 的阶的因子，所以 C_i 是 Z 的 n_i 阶子群．令 C 是 r 元组 $(c_1, c_2, \cdots, c_r)$ 所成的群，其中 $c_i\in C_i$，乘法按分量定义，则 C 是群 $C_1, C_2, \cdots, C_r$ 的(外)直积，而且 $C\cong A$ (参考卷1，中译本 p.134)．我们将得到 $\mathrm{Hom}(A, Z)$ 到 C 上的一个同构．为此，选取 A_i 的一个生成元 $a_i(i=1, 2, \cdots, r)$，如果 $\chi\in\mathrm{Hom}(A, Z)$，因为 $a_i^{n_i}=1$，则 $a_i^{\chi}=c_i$ 满足 $c_i^{n_i}=1$．于是 $c_i\in C_i$．现把 χ 映射到元素 $(c_1, c_2, \cdots, c_r)=(a_1^{\chi}, a_2^{\chi}, \cdots, a_r^{\chi})\in C$．如果 $\chi, \psi\in\mathrm{Hom}(A, Z)$，那末

$$\begin{aligned}(a_1^{\chi\psi}, \cdots, a_r^{\chi\psi}) &= (a_1^{\chi}a_1^{\psi}, \cdots, a_r^{\chi}a_r^{\psi})\\ &= (a_1^{\chi}, \cdots, a_r^{\chi})(a_1^{\psi}, \cdots, a_r^{\psi}),\end{aligned}$$

于是 $\chi\to(a_1^{\chi}, \cdots, a_r^{\chi})$ 是 $\mathrm{Hom}(A, Z)$ 到 C 内的一个同态．如果 $a_i^{\chi}=1(i=1, \cdots, r)$，由于 a_i 是 A 的生成元，故对每一 $a\in A$ 都有 $a^{\chi}=1$．于是由 $a_i^{\chi}=1$ (对一切 i) 推得 $\chi=1$．这就证明了 $\chi\to(a_1^{\chi}, \cdots, a_r^{\chi})$ 是到 C 内的同构．剩下要证明这个映射是满射：设 c_i 是 C_i 的任一元，则 $c_i^{n_i}=1$，而且显然有 A_i 到 C_i 上的同态 χ_i 使 $a_i^{\chi_i}=c_i$，因为 $A=A_1\times A_2\times\cdots\times A_r$，故映射

$x_1x_2\cdots x_r \to x_1^{\gamma_1}x_2^{\gamma_2}\cdots x_r^{\gamma_r}(x_i\in A_i)$ 是A到Z内的一个同态 χ。显然 $\chi\to(a_1^{\chi},\cdots,a_r^{\chi})=(c_1,c_2,\cdots,c_r)$，这表明了 $\mathrm{Hom}(A,Z)$ 到C的映射是满射。这就证明了 $A\cong C\cong \mathrm{Hom}(A,Z)$。

定理 6. 设A是有限交换群，Z是有限循环群，其阶被A的指数整除，则群 $\mathrm{Hom}(A,Z)$ 同构于A。

如果Z满足定理条件，那末称群 $\mathrm{Hom}(A,Z)$ 为群A的特征标群，其元称为A的特征标。

我们能迅速得到所需的特征标的结果，首先看如下的结论：

推论 1. 如果 $a\in A$，$a\neq 1$，则存在一个特征标 $\chi\in\mathrm{Hom}(A,Z)$，使 $a^{\chi}\neq 1$。

证　设B是A中对一切 $\chi\in\mathrm{Hom}(A,Z)$ 能使 $b^{\chi}=1$ 的元b所成子群。易见，若能证明 $B=1$，也就得到我们的结论。令 $\chi\in\mathrm{Hom}(A,Z)$，因为 $b^{\chi}=1$，$b\in B$，所以B在χ的核中，故有一个 A/B 到Z内的导出同态 $\bar\chi$，$\bar\chi$ 由 $(aB)^{\bar\chi}=a^{\chi}$ 定义。如果 $\chi,\phi\in\mathrm{Hom}(A,Z)$，而且 $\bar\chi=\bar\phi$，则由定义表明 $\chi=\phi$，所以 $\mathrm{Hom}(A,Z)$ 到 $\mathrm{Hom}(A/B,Z)$ 内的映射 $\chi\to\bar\chi$ 是1—1的。因为 $(A:1)=(\mathrm{Hom}(A,Z):1)$，$(A/B:1)=(\mathrm{Hom}(A/B,Z):1)$。由定理6知，这数必须相等，故 $B=1$。这就是我们所需要的。

如果a是A的一个固定元，则我们可以定义 $\mathrm{Hom}(A,Z)$ 到Z内的映射 $\eta_a:\chi^{\eta_a}=a^{\chi}$。如果 $\chi,\phi\in\mathrm{Hom}(A,Z)$，则有

$$(\chi\phi)^{\eta_a}=a^{\chi\phi}=a^{\chi}a^{\phi}=\chi^{\eta_a}\phi^{\eta_a},$$

所以 η_a 是 $\mathrm{Hom}(A,Z)$ 到Z内的一个同态，故 η_a 是群 $\mathrm{Hom}(A,Z)$ 的特征标。我们有基本的

推论 2. 对 $a\in A$，定义一个 $\mathrm{Hom}(A,Z)$ 到Z内的映射 η_a：$\chi^{\eta_a}=a^{\chi}$，则 $\eta_a\in\mathrm{Hom}(\mathrm{Hom}(A,Z),Z)$，而且映射 $a\to\eta_a$ 是A到 $\mathrm{Hom}(\mathrm{Hom}(A,Z),Z)$ 上的同构。

证　首先，由于 $\chi^{\eta_{ab}}=(ab)^{\chi}=a^{\chi}b^{\chi}=\chi^{\eta_a}\chi^{\eta_b}=\chi^{\eta_a\eta_b}$（最后的等式根据特征标群的乘积定义）可见 $a\to\eta_a$ 是同态。其次，设 $\eta_a=1$，则对一切 χ，$a^{\chi}=1$。于是由推论1知，$a=1$。这表明同态 $a\to\eta_a$ 的核只含恒等元，因此映射是一个同构。由定理6，

因为 $(A:1)=(\mathrm{Hom}(A, Z):1)=(\mathrm{Hom}(\mathrm{Hom}(A, Z), Z):1)$，故 $a\to\eta_a$ 是满射．证毕．

推论 2 允许我们把 A 和 $\mathrm{Hom}(A, Z)$（关于 Z）的特征标群等同起来，因此 A 和 $\mathrm{Hom}(A, Z)$ 之间有完全对偶性，以此证明

推论 3. 特征标集 $\{\chi_1, \chi_2, \cdots, \chi_r\}$ 生成特征标群 $\mathrm{Hom}(A, Z)$ 当且仅当满足 $a^{\chi_i}=1(i=1, 2, \cdots, r)$ 的 $a\in A$ 仅仅是 $a=1$．

证 这等价于对偶命题 $\{a_1, a_2, \cdots, a_r\}$ 生成 A 当且仅当使 $a_i^{\chi}=1(i=1, 2, \cdots, r)$ 成立的只有特征标 1．这是容易的；因为如果 $a_1, a_2, \cdots, a_r$ 生成 A 而且对特征标 χ，有 $a_i^{\chi}=1$ 成立，则因 χ 是同态而得到 $a^{\chi}=1$，这就推出 $\chi=1$．另一方面，如果 $a_1, a_2, \cdots, a_r$ 生成的子群是真子群，则存在 A/B 的特征标 $\bar{\chi}\neq 1$．若 $a\in A$，则映射 $a\to aB\to(aB)\bar{\chi}$ 是 $\mathrm{Hom}(A, Z)$ 中满足 $a_i^{\chi}=1(i=1, 2, \cdots, r)$ 而不为 1 的元．

3. 库默尔（Kummer）扩张 要得到给定域 Φ 上的阿贝尔扩张的全貌往往是困难的．比如，Φ 是有理数域时，就需要深入的数论研究．但是有两类阿贝尔扩张可以用比较初等的代数方法加以十分详尽的研究．其一是所谓阿贝尔 p 扩张，即特征 $p\neq 0$ 的域上 p^e 维阿贝尔扩张，这将在 § 5 中讨论．本节叙述库默尔扩张理论，其定义如下

定义 1. 设 P 是域 Φ 的一个阿贝尔扩张，称 P/Φ 为库默尔 m 扩张，如果 P/Φ 的伽罗瓦群的指数为 m，并且 Φ 含 m 个不同的 m 次单位根．

假设 Φ 是包含 m 个不同的 m 次单位根的给定域，在整个讨论中，域 Φ 和整数 m 是固定的我们希望得到库默尔 m' 扩张 P/Φ 的概括认识，此处 $m'|m$．已经知道，由 Φ 含 m 个不同的 m 次单位根可以推出其特征不是 m 的因子（§ 2.2）．如果 P/Φ 是库默尔 m' 扩张，$m'|m$，则 $[\mathrm{P}:\Phi]=(G:1)$，由于有限交换群的指数和阶被同样的素数整除，可见特征不是 $[\mathrm{P}:\Phi]$ 的因子．

Φ 和 m 如上所示，P/Φ 是库默尔 m' 扩张，$m'|m$，而 P^* 和 Φ^*

分别是 P 和 Φ 的非零元的乘群. 对于 $\rho\in P^*$, 映射 $\rho\to\rho^m$ 是 P^* 的自同态,它把 Φ^* 映射到自身内. $\rho\to\rho^m$ 的核是 m 次单位根作成的 m 阶群 $Z(m)$, 而且 $Z(m)\subseteq\Phi^*$. 令

$$M(P)=\{\rho\in P^*|\rho^m\in\Phi^*\}. \tag{7}$$

$$N(P)=\{\rho^m|\rho\in M(P)\}. \tag{8}$$

则 $M(P)$ 是由 Φ^* 的元在 P 中的 m 次根组成,而 $N(P)$ 是 Φ^* 中元的集,这些元是 P 的元的 m 次幂. 显然 $M(P)$ 是 P^* 中包含 Φ^* 的子群, $N(P)$ 是 Φ^* 中包含 $\Phi^{*m}=\{\alpha^m|\alpha\in\Phi^*\}$ 的子群.

设 $\rho\in M(P)$, 令 $\chi_\rho(s)=\rho^s\rho^{-1}$, $s\in G$. 因为 $\rho^m=\alpha\in\Phi$, $(\rho^s)^m=\alpha$, 于是 $\rho^s\rho^{-1}\in Z(m)$. 但因 $Z(m)\subseteq\Phi$,

$$\chi_\rho(st)=\rho^{st}\rho^{-1}=(\rho^t\rho^{-1})^s(\rho^t\rho^{-1})=\chi_\rho(s)\chi_\rho(t).$$

可见 $\chi_\rho\in \mathrm{Hom}(G,Z)$, $Z=Z(m)$. 因为 G 的指数是 m 的因子,所以 $\mathrm{Hom}(G,Z)$ 是有限交换群 G 的特征标群. 反之, 设 χ 是 $\mathrm{Hom}(G,Z)$ 的任意一个元,则 $\chi(st)=\chi(s)\chi(t)=\chi(s)^t\chi(t)$, 满足诺德方程. 因此由诺德定理 (定理 1.19), 存在非零元 $\rho\in P$ 使得 $\chi(s)=\rho^s\rho^{-1}$. 因为 $\rho^s\rho^{-1}\in Z$, 于是对每一 $s\in G$ 有

$$(\rho^s)^m=\rho^m \text{ 或 } (\rho^m)^s=\rho^m.$$

故 $\rho^m\in\Phi$, 从而 $\rho\in M(P)$.这样,我们就证明了特征标群 $\mathrm{Hom}(G,Z)$ 的每一元有如下的形式 $\chi(s)=\rho^s\rho^{-1}$, ρ 在 $M(P)$ 中. 如果 $\rho_1,\rho_2\in M(P)$, 而且 $\chi_{\rho_1},\chi_{\rho_2}$ 是 G 的相应的特征标,则

$$\begin{aligned}\chi_{\rho_1\rho_2}(s)&=(\rho_1\rho_2)^s(\rho_1\rho_2)^{-1}=\rho_1^s\rho_1^{-1}\rho_2^s\rho_2^{-1}\\&=\chi_{\rho_1}(s)\chi_{\rho_2}(s).\end{aligned}$$

因此映射 $\rho\to\chi_\rho(s)$ 是 $M(P)$ 到 $\mathrm{Hom}(G,Z)$ 上的同态. 此同态的核是适合 $\rho^s\rho^{-1}=1$, $s\in G$ 的元 $\rho\in M(P)$ 的集, 这恰是满足 $\rho^s=\rho$, $s\in G$ 的元 $\rho\neq 0$ 的集,故是 Φ^*.

把刚才得到的关于 $M(P)$ 到 $\mathrm{Hom}(G,Z)$ 上的同态的结果用群同态的正合序列来陈述是很方便的. 设 $G_1, G_2,\cdots,G_k$ 是群, η_i 是群 G_i 在 G_{i+1} 内的同态,我们称序列

$$G_1\underset{\eta_1}{\to}G_2\underset{\eta_2}{\to}\cdots\to G_{k-1}\underset{\eta_{k-1}}{\to}G_k$$

是正合的，如果对每一 $i=1,2,\cdots,k-2$，G_i 在 η_i 下的象与 η_{i+1} 的核重合．如果 1 表示仅由单位元 1 组成的群，则 1 到任意群内的同态只有 $1\longrightarrow 1$．由此及正合性的定义得到：$1\to G_1\xrightarrow[\eta]{}G_2$ 是正合的，当且仅当 η 是 1-1 的；$G_1\xrightarrow[\eta]{}G_2\to 1$ 是正合的，当且仅当 η 是满射．

利用这些术语，我们可叙述以下定理．

定理 7. 设 Φ 是含 m 个不同的 m 次单位根的域，P/Φ 是库默尔 m' 扩张，$m'|m$，$M(\mathrm{P})$ 由 (7) 所定义，其中 P^* 是 P 的乘法群，Φ^* 是 Φ 的乘法群，则有乘法群的正合序列

$$1\to\Phi^*\to M(\mathrm{P})\to \mathrm{Hom}(G,Z)\to 1,$$

这里 Φ^* 的同态是包含映射，$M(\mathrm{P})$ 的同态是 $\rho\to\chi_\rho$，$\chi_\rho(s)=\rho^s\rho^{-1}$．商群 $M(\mathrm{P})/\Phi^*$[1)]有限且同构于 G．还有 $\mathrm{P}=\Phi(M(\mathrm{P}))$，并且 $\mathrm{P}=\Phi(\rho_1,\rho_2,\cdots,\rho_r)$，$\rho_i\in M(\mathrm{P})$ 的充要条件是陪集 $\rho_i\Phi^*$ 生成 $M(\mathrm{P})/\Phi^*$．

证　所给序列的正合性的第一个命题是指 Φ^* 是映射 $\rho\to\chi_\rho$ 的核，而且这个映射是 $\mathrm{Hom}(G,Z)$ 上的满射．对于这两点上面已经给予证明，于是有 $\mathrm{Hom}(G,Z)\cong M(\mathrm{P})/\Phi^*$．因为

$$\mathrm{Hom}(G,Z)\cong G,$$

由定理 6，有 $M(\mathrm{P})/\Phi^*\cong G$．这就证明了第二个命题．现在设 $\rho_1,\rho_2,\cdots,\rho_r$ 是 $M(\mathrm{P})$ 的使得陪集 $\rho_i\Phi^*$ 生成有限群 $M(\mathrm{P})/\Phi^*$ 的元，显然 $M(\mathrm{P})$ 的同态 $\rho\to\chi_\rho$ 给出了 $M(\mathrm{P})/\Phi^*$ 到 $\mathrm{Hom}(G,Z)$ 上的同构 $\rho_\Phi^*\to\chi_\rho$，因此特征标 χ_{ρ_i} 生成 $\mathrm{Hom}(G,Z)$．今设 $\mathrm{P}'=\Phi(\rho_1,\rho_2,\cdots,\rho_r)$，$H$ 是 G 的相应于 P' 的子群 (P/P' 的伽罗瓦群)．如果 $t\in H$，则有 $\rho_i^t=\rho_i$，$1\leqslant i\leqslant r$，于是 $\chi_{\rho_i}(t)=1$．这就推出，对每一 $\chi\in\mathrm{Hom}(G,Z)$ 有 $\chi(t)=1$．再由定理 6 的推论 1 得到 $t=1$．因此 $H=1$，从而得到 $\mathrm{P}'=\Phi(\rho_1,\rho_2,\cdots,\rho_r)=\mathrm{P}$，$\mathrm{P}=\Phi(M(\mathrm{P}))$．反之，设 $\rho_1,\rho_2,\cdots,\rho_r\in M(\mathrm{P})$ 满足

1) 原文误为 $M(\mathrm{P})/\mathrm{P}^*$．——译者注．

$\Phi(\rho_1, \rho_2, \cdots, \rho_r) = \mathrm{P}$，且 $s \in G$，则由 $\rho_i^s = \rho_i$，$1 \leqslant i \leqslant r$，推出 $\rho^s = \rho$，$\rho \in \mathrm{P}$. 可见从 $\chi_{\rho_i}(s) = 1$，$1 \leqslant i \leqslant r$ 可推出 $s = 1$. 因此由定理6的推论3得到χ_{ρ_i}生成 $\mathrm{Hom}(G, Z)$. 特别地当 $\rho \in M(\mathrm{P})$ 时，有 $\chi_\rho = \chi_{\rho_1}^{k_1}\chi_{\rho_2}^{k_2}\cdots\chi_{\rho_r}^{k_r}$. 于是对每一 $s \in G$ 都有

$$\rho^s\rho^{-1} = (\rho_1^s\rho_1^{-1})^{k_1}(\rho_2^s\rho_2^{-1})^{k_2}\cdots(\rho_r^s\rho_r^{-1})^{k_r}$$

因此，$(\rho\rho_1^{-k_1}\rho_2^{-k_2}\cdots\rho_r^{-k_r})^s = \rho\rho_1^{-k_1}\rho_2^{-k_2}\cdots\rho_r^{-k_r}$，$s \in G$. 于是

$$\rho = \beta\rho_1^{k_1}\cdots\rho_r^{k_r},$$

$\beta \in \Phi^*$，由于ρ是 $M(\mathrm{P})$ 的任一元，这就证明了陪集 $\rho_i\Phi^*$ 生成 $M(\mathrm{P})/\Phi^*$. 证毕.

下面考虑 $M(\mathrm{P})$ 到商群 $N(\mathrm{P})/\Phi^{*m}$ 上的映射 $\rho \to \rho^m\Phi^{*m}$. 这是一个同态，其核是 $M(\mathrm{P})$ 中满足 $\rho^m = \alpha^m(\alpha \in \Phi^*)$ 的元ρ的集. 那末 $\rho = \zeta\alpha$，此处 $\zeta^m = 1$. 因为 $Z \subseteq \Phi^*$，这些ρ恰好是Φ^*的元，因此有 $M(\mathrm{P})/\Phi^*$ 到 $N(\mathrm{P})/\Phi^{*m}$ 上的同构 $\rho\Phi^* \to \rho^m\Phi^{*m}$. 因为 $M(\mathrm{P})/\Phi^*$ 同构于 P/Φ 的伽罗瓦群，显然 $N(\mathrm{P})/\Phi^{*m}$ 是 Φ^*/Φ^{*m} 的有限子群，而且有

$$N(\mathrm{P})/\Phi^{*m} \cong M(\mathrm{P})/\Phi^* \cong G. \tag{9}$$

现在把注意力转移到Φ^*的子群 $N(\mathrm{P})$ 上，它满足两个条件：$N(\mathrm{P}) \supseteq \Phi^{*m}$ 及 $N(\mathrm{P})/\Phi^{*m}$ 是有限的. 我们将看到，这些由Φ和m决定的子群能用来给出库默尔扩张 P/Φ 的概貌. 首先，如果 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 $N(\mathrm{P})$ 的元，使得陪集 $\alpha_i\Phi^{*m}$ 生成 $N(\mathrm{P})/\Phi^{*m}$，则P/Φ是

$$f(x) = (x^m - \alpha_1)(x^m - \alpha_2)\cdots(x^m - \alpha_r)$$

的分裂域. 因为有 $\rho_i^m = \alpha_i$，$(\rho_i \in M(\mathrm{P}))$，以及由 $M(\mathrm{P})/\Phi^*$ 和 $N(\mathrm{P})/\Phi^{*m}$ 的同构 $\rho\Phi^* \to \rho^m\Phi^{*m}$，推出陪集$\rho_i\Phi^*$生成 $M(\mathrm{P})/\Phi^*$. 因此由定理7得到 $\mathrm{P} = \Phi(\rho_1, \cdots, \rho_r)$. 如果 $Z = \{\zeta_j\}$，则 $f(x)$ 的根是 $\rho_i\zeta_j$，可见 $\mathrm{P} = \Phi(\rho_i\zeta_j)$ 是 $f(x)$ 在Φ上的分裂域.

其次着手证明 Φ^* 中满足上述条件的任意子群N可由库默尔扩张得到. 精确结果如下：

定理 8. 设Φ是包含m个不同的m次单位根的域，N是 Φ^* 中含 Φ^{*m} 的子群且使 N/Φ^{*m} 有限，则存在库默尔 $m' \to$ 扩张

P/Φ, $m'|m$, 使 $N(\mathrm{P})=N$, 其中 $N(\mathrm{P})$ 和 $M(\mathrm{P})$ 由 (8) 和 (7) 所定义.

证　上面关于库默尔扩张的分析给出定义 P/Φ 的线索,鉴于这一点,导致我们在所给群 N 中选择 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 使陪集 $\alpha_i\Phi^{*m}$ 生成 N/Φ^{*m}. 令 P/Φ 是 (10) 中给定的多项式 $f(x)$ 的分裂域. 因为 $x^m-\alpha_i$ 有 m 个不同的根,所以 $f(x)$ 是可分的, 而且 P/Φ 是有限维伽罗瓦域. 设 G 是伽罗瓦群, 如果 ρ_i 是 $x^m-\alpha_i$ 的根, 则这个多项式的所有根是 $\rho_i\zeta_j$, ζ_j 在 m 次单位根的群 Z 中. 因此, 如果 $s\in G$, 则 $\rho_i^s=\zeta_i(s)\rho_i$, $\zeta_i(s)\in Z$. 如果 $s, t\in G$, 则有

$$\begin{aligned}\rho_i^{st}&=(\zeta_i(s)\rho_i)^t=\zeta_i(s)\rho_i^t\\&=\zeta_i(s)\zeta_i(t)\rho_i,\end{aligned}$$

因此 $\rho_i^{st}=\rho_i^{ts}(i=1, 2,\cdots, r)$, 又因为显然有 $\mathrm{P}=\Phi(\rho_1, \rho_2, \cdots, \rho_r)$, 且对一切 $s, t\in G$, 有 $st=ts$, 这就证明了 G 是交换群. 又因为 $\rho_i^{s^k}=\zeta_i(s)^k\rho_i$, $k=1, 2,\cdots$, 于是 $\rho_i^{s^m}=\rho_i$, 这就推出对于 $s\in G$ 有 $s^m=1$, 因此 G 的指数是 m 的因子. 又因 $Z\subseteq\Phi$, 所以 P/Φ 是库默尔 m' 扩张. 剩下要证明, 若 $N(\mathrm{P})$ 如 (8) 所定义,则 $N(\mathrm{P})=N$. 因为 $\rho_i^m=\alpha_i\in\Phi$, $\rho_i\in M(\mathrm{P})$, 由 (7) 定义. 由于 $\mathrm{P}=\Phi(\rho_1,\cdots, \rho_r)$, 定理 7 表明陪集 $\rho_i\Phi^*$ 生成 $M(\mathrm{P})/\Phi^*$. 应用 $M(\mathrm{P})/\Phi^*$ 和 $N(\mathrm{P})/\Phi^{*m}$ 的同构, 就知道 $\alpha_i\Phi^{*m}$ 生成 $N(\mathrm{P})/\Phi^{*m}$. 另一方面,我们知道陪集 $\alpha_i\Phi^{*m}$ 生成 N/Φ^{*m}, 这就推出 $N(\mathrm{P})=N$.

现在考虑两个库默尔 m_i 扩张 $\mathrm{P}_i/\Phi(i=1, 2, m_i|m)$. 从 $M(\mathrm{P}_i)$ 和 $N(\mathrm{P}_i)$ 的定义, 显然可知, 如果 $\mathrm{P}_1/\Phi\cong\mathrm{P}_2/\Phi$, 则 Φ^* 的子群 $N(\mathrm{P}_1)$ 和 $N(\mathrm{P}_2)$ 重合. 反之, 假若 $N(\mathrm{P}_1)=N(\mathrm{P}_2)$, 我们已看到,如果 $\alpha_1, \alpha_2,\cdots, \alpha_r$ 是 $N(\mathrm{P}_i)$ 的元, 使陪集 $\alpha_i\Phi^{*m}$ 生成 $N(P_i)/\Phi^{*m}$, 则 P_i 是 $f(x)=(x^m-\alpha_1)(x^m-\alpha_2)\cdots(x^m-\alpha_r)$ 在 Φ 上的分裂域. 由分裂域的唯一性得到, 当 $N(\mathrm{P}_1)=N(\mathrm{P}_2)$ 时, $\mathrm{P}_1/\Phi\cong\mathrm{P}_2/\Phi$. 以下考察含于某一扩张域 Ω/Φ (例如 § 4.1 意义下 Φ 的代数闭包)中的库默尔 m' 扩张 P/Φ, $m'|m$. 已经知道, 如果 P_i/Φ 是扩张之一,则 $\mathrm{P}_i=\Phi(M(\mathrm{P}_i))$. 因此,显然有, $\mathrm{P}_1\supseteq$

P_2当且仅当 $M(P_1)\supseteq M(P_2)$，同样显然有 $M(P_1)\supseteq M(P_2)$ 当且仅当 $N(P_1)\supseteq N(P_2)$；于是 $P_1\supseteq P_2$ 当且仅当 $N(P_1)\supseteq N(P_2)$。显然，我们借助 Φ^* 中满足 $N\supseteq\Phi^{*m}$ 及 N/Φ^{*m} 有限这两个条件的子群 N，对库默尔扩张 P/Φ 的内部性质给出了令人满意的描述。

习　题　24

1. 证明：有理数域有无限多个不同构的二次扩张.

2. 设Φ包含m个不同的m次单位根，P/Φ 是Φ上的m维循环扩张，P/Φ 的伽罗瓦群的生成元为 s. 证明 $P=\Phi(\rho)$，其中 $\rho^m=\alpha\in\Phi$，$\rho^s=\zeta\rho$，ζ是m次本原单位根. 并证明：如果$\sigma\in P$ 满足 $\sigma^m\in\Phi$，则 $\sigma=\beta\rho^k$，$\beta\in\Phi$，$1\leqslant k\leqslant m$.

3. (阿尔伯特 (Albert)) 设P是Φ上 $n=l^e$ 维循环(扩张)，其中l是素数，而且Φ含包l个不同的l次单位根. 令s是 P/Φ 的伽罗瓦群G的生成元，H是由$t=s^m(m=l^{e-1})$ 生成的G之l阶子群，E是H不变元的子域，于是 E/Φ 是 P/Φ 中唯一的m维子域. 由第2题，$P=E(\rho)$，此处 $\rho^l=\alpha\in E$，$\rho^t=\zeta\rho$，ζ 是l次本原单位根. 证明 $\rho^s=\beta\rho^k$，$\beta\in E$，$1\leqslant k<l$，并证明 $\rho^t=\gamma\rho^{k^m}=\zeta\rho$，其中 $\gamma\in E$，因而 $k^m\equiv 1(\mathrm{mod}\,l)$，$k=1$. 再证明 $N_{E|\Phi}(\beta)=\zeta$，$\alpha^s\alpha^{-1}=\beta^l$.

4. (阿尔伯特)设Φ有l个不同的l次单位根，l是素数. E/Φ 是Φ上 $m=l^{e-1}$ 维循环扩张，$e>1$. 假设E含元β使 $N_{E|\Phi}(\beta)=\zeta$ 是l次本原单位根. 证明存在 $\alpha\in E$使 $\alpha^s\alpha^{-1}=\beta^l$，其中$s$是$E/\Phi$ 的伽罗瓦群的生成元. 证明α不是E中的一个l次幂，于是当 $P=E(\rho)$，$\rho^l=\alpha$ 时，有 $[P:E]=l$. 再证P是Φ上l^e 维循环扩张.

5. 由第3题和第4题可推得以下结果：如果Φ包含l个不同的l次单位根，l是素数，E/Φ 是 $l^f>1$ 维循环扩张，则 E/Φ 能嵌入一个 l^{f+1} 维循环扩张P/Φ中当且仅当l次本原单位根ζ是E的一个元素的范数. 由此证明，如果Φ的特征$\neq 2$，二次扩张 $E=\Phi(\varepsilon)$，$(\varepsilon^2=\gamma\in\Phi)$ 能嵌入Φ的二次循环扩张当且仅当γ是Φ的两个元之平方和. 特别地，如果 R_0 是有理数域，则虚二次扩张 $R_0(\varepsilon)$ 不能嵌入四次循环扩张中，其中 $\varepsilon^2=r<0$，$r\in R_0$.

6. (妥特)令P是R_0上的p次单位根的域，p是形如 $4n+1$ 的素数，证明P包含一个实二次子域.

7. 假若Φ包含四个不同的4次单位根. 证明任何二次扩张 E/Φ 能嵌入四次循环扩张 P/Φ 中.

4. 维特 (Witt) 向量　我们曾经定义特征 $p\neq 0$ 的域Φ的阿贝尔p扩张是Φ的 p^e 维阿贝尔扩张. p维和p^2维循环p扩张首先是阿廷和施莱尔在与实域有关的一个问题上遇到的(参看§6.9)，阿尔伯特推广了他们的构造，给出了一个p^e维循环p扩张的归纳

构造.稍后,维特给出一个直接构造,并按照刚刚讨论过的库默尔扩张理论的线索,给出了阿贝尔 p 扩张的概述.维特的方法建基于一个确定在特征为 p 的给定域上向量环的巧妙定义之上，这个构造在其它方面(例如赋值论)亦有重要应用.现在来论述其一般形式.

首先从有理数域 R_0 上的未定元 x_i, y_j, $z_k(i, j, k=0, 1, \cdots, m-1)$ 的多项式环 $\mathfrak{X}=R_0[x_i, y_j, z_k]$ 开始. 令 $\mathfrak{X}^{(m)}$ 是 m 元组 $(a_0, a_1, \cdots, a_{m-1})$ 集, $a_i \in \mathfrak{X}$, 按惯例用分量定义其相等、加法与乘法: 设 $a=(a_0, \cdots, a_{m-1})$, $b=(b_0, \cdots, b_{m-1})$, 它们的和与积记作 $a \oplus b$, $a \odot b$, 那么, $a \oplus b=(a_0+b_0, \cdots, a_{m-1}+b_{m-1})$, $a \odot b=(a_0 b_0, \cdots, a_{m-1} b_{m-1})$. 令 p 是一个固定的素数,以此按下面规则定义 $\mathfrak{X}$ 的映射 φ: 如果 $a=(a_0, a_1, \cdots, a_{m-1})$ 则 $a^{\varphi}=(a^{(0)}, a^{(1)}, \cdots, a^{(m-1)})$, 此处

$$a^{(\nu)}=a_0^{p^\nu}+p a_1^{p^{\nu-1}}+\cdots+p^\nu a_\nu \quad (\nu=0,1, \cdots, m-1). \tag{11}$$

于是 $a^{(0)}=a_0$, $a^{(1)}=a_0^p+p a_1$, $\cdots$. 我们又引入映射 $\mathrm{P}: a \rightarrow a^p=(a_0^p, a_1^p, \cdots, a_{m-1}^p)$, 则定义 (11) 给出

$$a^{(0)}=a_0, \quad a^{(\nu)}=(a^p)^{(\nu-1)}+p^\nu a_\nu(\nu \geqslant 1). \tag{12}$$

其次,令 $A=(a^{(0)}, a^{(1)}, \cdots, a^{(m-1)})$ 是任意元素,定义一个映射 ψ: $A^\psi=(a_0, a_1, \cdots, a_{m-1})$, 此处

$$a_0=a^{(0)},$$

$$a_\nu=\frac{1}{p^\nu}(a^{(\nu)}-a_0^{p^\nu}-p a_1^{p^{\nu-1}}-\cdots-p^{\nu-1} a_{\nu-1}) \quad (\nu \geqslant 1). \tag{13}$$

直接验算可得 $a^{\varphi\psi}=a$, $A^{\psi\varphi}=A$, 这就证明了 φ 是以 ψ 为逆的双射.

现在用映射 φ 和 $\psi=\varphi^{-1}$ 定义 $\mathfrak{X}^{(m)}$ 的一个新的加法合成和乘法合成,分别定义

$$\begin{aligned} a+b &=(a^{\varphi} \oplus b^{\varphi})^{\varphi^{-1}}, \\ a b &=(a^{\varphi} \odot b^{\varphi})^{\varphi^{-1}}. \end{aligned} \tag{14}$$

这些提供了 $\mathfrak{X}^{(m)}$ 的另一个环结构(卷 1,中译本 p.68, 习题的第

6题). 将新的环记作 $\mathfrak{X}_m$, 则 $\mathfrak{X}_m$ 和 $\mathfrak{X}^{(m)}$ 作为集合是相同的, $a \to a^\varphi$ 是 $\mathfrak{X}_m$ 到 $\mathfrak{X}^{(m)}$ 上的一个同构,因此 $\mathfrak{X}_m$ 和 $\mathfrak{X}^{(m)}$ 一样是交换环.

现在考查关于"一般"向量 $x=(x_0, x_1, \cdots, x_{m-1})$ 和 $y=(y_0, y_1, \cdots, y_{m-1})$ 的 $x+y$, xy 和 $x-y$ 的公式,其中 x_i, y_i 是未定元. 例如有

$$(x+y)_0 = x_0 + y_0,$$

$$(x+y)_1 = x_1 + y_1 - \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}x_0^i y_0^{p-i},$$

$$(xy)_0 = x_0 y_0, \quad (xy)_1 = x_0^p y_1 + x_1 y_0^p + p x_1 y_1.$$

一般地,如果用 $\circ$ 表示合成+, $\cdot$, −中的任意一种,显然从定义得到 $x\circ y$ 的第 ν 个分量 $(x\circ y)_\nu$ 是 x_0, y_0, x_1, y_1, $\cdots$, $x_\nu y_\nu$ 的有理系数多项式. 也容易看出

$$(x+y)_\nu = x_\nu + y_\nu + f_\nu(x_0, y_0, \cdots, x_{\nu-1}, y_{\nu-1}) \tag{15}$$

此处 f_ν 是所指定的未定元的多项式, 我们将要建立的基本结果是 $(x\circ y)_\nu$ 为 x_0, y_0, $\cdots$, $x_\nu y_\nu$ 的整系数多项式.

在整个讨论中,如果 $a=(a_0, a_1, \cdots, a_{m-1})$, 则记

$$a^\varphi = (a^{(0)}, a^{(1)}, \cdots, a^{(m-1)})$$

等等. 令 $I[x_i, y_i]$ 是 x_0, y_0, $\cdots$, x_{m-1}, y_{m-1} 的系数在整数环 I 内的多项式环. 若 μ 是非负整数, 则我们用 (p^μ) 表示理想 $p^\mu I[x_i, y_i]$, 如果 $c-d\in(p^\mu)$ 就写成 $c\equiv d(p^\mu)$ 则有

引理 1. 令 $\mu\geqslant 1$, $0\leqslant k\leqslant m-1$, $a=(a_\nu)$, $b=(b_\nu)$, $0\leqslant\nu\leqslant m-1$, a_ν, $b_\nu\in I[x_i, y_i]$. 记 $a^\varphi=(a^{(\nu)})$, $b^\varphi=(b^{(\nu)})$, 则同余式组

$$a_\nu\equiv b_\nu(p^\mu), \quad 0\leqslant\nu\leqslant k \tag{16}$$

等价于

$$a^{(\nu)}\equiv b^{(\nu)}(p^{\mu+\nu}), \quad 0\leqslant\nu\leqslant k. \tag{17}$$

证. 我们有 $a^{(0)}=a_0$, $b^{(0)}=b_0$, 所以当 $k=0$ 时结果是显然的. 对 k 作归纳来证明: 假设 $0\leqslant\nu\leqslant k-1$ 时, (16) 和 (17) 同时成立. 在这些条件下证明 $a_k\equiv b_k(p^\mu)$ 当且仅当

$$a^{(k)}\equiv b^{(k)}(p^{\mu+k}).$$

显然 $a_k \equiv b_k(p^\mu)$ 当且仅当 $p^k a_k \equiv p^k b_k(p^{\mu+k})$. 因此利用 (12), 只要在归纳假设下证明 $(a^p)^{(k-1)} \equiv (b^p)^{k-1}(p^{\mu+k})$ 即可. 我们有 $a_\nu \equiv b_\nu(p^\mu)(0 \leqslant \nu \leqslant k-1)$. 利用 $\binom{p}{i} \equiv 0(p)$, $(1 \leqslant i \leqslant p-1)$, 得到 $a_\nu^p \equiv b_\nu^p(p^{\mu+1})$, $(0 \leqslant \nu \leqslant k-1)$. 将关于 k 的归纳假设用于 a^p 与 b^p 得出 $(a^p)^{(k-1)} \equiv (b^p)^{(k-1)}(p^{\mu+1+k-1})$, 这就是所要求的.

现在我们可以证明基本的

定理 9. 如果 $x \circ y$ 表示 $x+y$, xy 或 $x-y$, 则 $(x \circ y)_\nu$ 是 $x_0, y_0, x_1, y_1, \cdots, x_\nu, y_\nu$ 的整系数多项式.

证 因为 $(x \circ y)_\nu$ 是 $x_0, y_0, \cdots, x_\nu y_\nu$ 的有理系数多项式, 只要证明 $(x \circ y)_\nu \in I[x_i, y_i]$ 就行了. $(x \circ y)_0 \in I[x_i, y_i]$ 是显然的, 假设对 $0 \leqslant k \leqslant \nu-1$, $(x \circ y)_k \in I[x_i, y_i]$, 由 (12) 得到

$$p^\nu (x \circ y)_\nu = (x \circ y)^{(\nu)} - ((x \circ y)^p)^{(\nu-1)}, \tag{18}$$

而且 $(x \circ y)^{(\nu)} = x^{(\nu)} \dot{\pm} y^{(\nu)} \in I[x_i, y_i]$, 由归纳假设推出

$$((x \circ y)^p)_{(\nu-1)} \in I[x_i, y_i].$$

因此由 (18), 只要证明 $(x \circ y)^{(\nu)} \equiv ((x \circ y)^p)^{(\nu-1)}(p^\nu)$. 由 (12) 有 $x^{(\nu)} \equiv (x^p)^{(\nu-1)}(p^\nu)$, $y^{(\nu)} \equiv (y^p)^{(\nu-1)}(p^\nu)$, 因此

$$\begin{aligned}(x \circ y)^{(\nu)} = x^{(\nu)} \dot{\pm} y^{(\nu)} &\equiv (x^p)^{(\nu-1)} \dot{\pm} (y^p)^{(\nu-1)} \\ &\equiv (x^p \circ y^p)^{(\nu-1)}(p^\nu).\end{aligned} \tag{19}$$

我们假设 $(x \circ y)_k \in I[x_i, y_i]$, $0 \leqslant k \leqslant \nu-1$. 对任何整系数多项式有 $f(x_0, y_0, \cdots)^p \equiv f(x_0^p, y_0^p, \cdots)(p)$. 于是

$$(x \circ y)_k^p \equiv (x^p \circ y^p)_k(p), \quad 0 \leqslant k \leqslant \nu-1,$$

因此由引理 1 得到

$$((x \circ y)^p)^{(\nu-1)} \equiv (x^p \circ y^p)^{(\nu-1)}(p^\nu). \tag{20}$$

由 (19) 和 (20), $(x \circ y)^{(\nu)} \equiv ((x \circ y)^p)^{(\nu-1)}(p^\nu)$. 证毕.

为了方便起见, 将已经得到的结果罗列于后:

$$\begin{aligned}&(x+y)_\nu = s_\nu(x_0, y_0, \cdots, x_\nu y_\nu) \in I[x_i, y_i], \\ &(xy)_\nu = m_\nu(x_0, y_0, \cdots, x_\nu, y_\nu) \in I[x_i, y_i],\end{aligned} \tag{21}$$

$$(x-y)_\nu = d_\nu(x_0, y_0, \cdots, x_\nu, y_\nu) \in I[x_i, y_i].$$

我们还注意到，$(0,\cdots,0)$ 和 $(1,\cdots,1)$ 是 $\mathfrak{X}^{(m)}$ 的零元和恒等元，$(0,\cdots,0)^\varphi=(0,\cdots,0)$，$(1,0,\cdots,0)^\varphi=(1,\cdots,1)$，则 $(0,\cdots,0)$ 和 $(1,0,\cdots,0)$ 是 $\mathfrak{X}_m$ 的零元和恒等元。令 η 是 R_0 上 $\mathfrak{X}$ 到自身内的代数同态，假设 $x_\nu^\eta=a_\nu$，$y_\nu^\eta=b_\nu$，$0\leqslant\nu\leqslant m-1$，则 $(x^{(\nu)})^\eta=a^{(\nu)}$，$(y^{(\nu)})^\eta=b^{(\nu)}$，$((x+y)^{(\nu)})^\eta=a^{(\nu)}+b^{(\nu)}$，

$$((x+y)_\nu)^\eta=(a+b)_\nu.$$

因此，由 (21) 得到：$(a+b)_\nu=S_\nu(a_0, b_0, \cdots, a_\nu, b_\nu)$，类似的公式对 $(ab)_\nu$ 和 $(a-b)_\nu$ 也成立．因为存在 R_0 上 $\mathfrak{X}$ 的同态 η 使 x_ν^η 和 y_ν^η 是 $\mathfrak{X}$ 的任意元，所以这些公式对一切 $a, b\in\mathfrak{X}_m$ 都成立．显然，由这些公式推出如果 $\mathfrak{B}$ 是 $R_0[x_i, y_i, z_k]$ 的任一子环，则满足 $b_\nu\in\mathfrak{B}$ 的向量 $(b_0, b_1, \cdots, b_{m-1})$ 的集 $\mathfrak{B}$ 是 $\mathfrak{X}_m$ 的子环．尤其是，对 $\mathfrak{B}=\mathfrak{Y}\equiv I[x_i, y_i, z_k]$ 和 $\mathfrak{B}=\mathfrak{Y}'\equiv I[x_i, y_i]$ 的情形是成立的。

现在来定义维特向量环 $\mathfrak{W}_m(\mathfrak{A})$．这里 $\mathfrak{A}$ 是 p 个元的域 I_p 上的交换代数，p 是上面用过的素数。$\mathfrak{W}_m(\mathfrak{A})$ 的元是"向量" $(a_0, a_1, \cdots, a_{m-1})$，这里 $a_\nu\in\mathfrak{A}$．相等是按通常方法定义的．如果 $a=(a_0, a_1, \cdots, a_{m-1})$，$b=(b_0, b_1, \cdots, b_{m-1})$，那末在 $\mathfrak{W}_m(\mathfrak{A})$ 中加法和乘法可定义为

$$(a+b)_\nu=\bar{s}_\nu(a_0, b_0, \cdots, a_\nu, b_\nu), \tag{22}$$
$$(ab)_\nu=\bar{m}_\nu(a_0, b_0, \cdots, a_\nu, b_\nu),$$

这里，$a+b=((a+b)_0, \cdots, (a+b)_{m-1})$，$ab=((ab)_0, \cdots, (ab)_{m-1})$。如果 $f(x_0, y_0, \cdots)$ 是整系数多项式，则 $\bar{f}(a_0, a_1, \cdots)$ 是 $\mathfrak{A}$ 的元，它是将 $f(x_0, y_0, \cdots)$ 的整系数以其在 I_p 中的陪集代替，x_ν 用 a_ν，y_ν 用 b_ν 代替 $(0\leqslant\nu\leqslant m-1)$ 而得到．这些替换相当于运用 $I[x_i, y_i]$ 到 $\mathfrak{A}$ 内的同态：$n\to\bar{n}=n+(p)$，$n\in I$，$x_\nu\to a_\nu$，$y_\nu\to b_\nu$。

今设 $a=(a_\nu)$，$b=(b_\nu)$，$c=(c_\nu)$是 $\mathfrak{W}_m(\mathfrak{A})$ 的任意三个元，我们有 $I[x_i, y_i, z_k]$ 到 $\mathfrak{A}$ 内的同态，使 $n\to\bar{n}$，$n\in I$，$x_\nu\to a_\nu$，$y_\nu\to b_\nu$，$z_\nu\to c_\nu$．考察向量 $(w_0, w_1, \cdots, w_{m-1})$ 作成的 $\mathfrak{X}_m$

的子环$\mathfrak{S}_m$，其中 $w_\nu \in I[x_i, y_i, z_k]$. 已知当 $t=(t_0, \cdots, t_{m-1}) \in \mathfrak{S}_m$ 时，$(w+t)_\nu = s_\nu(\omega_0, t_0, \cdots, \omega_\nu, t_\nu)$，$(\omega t)_\nu = m_\nu(\omega_0, t_0, \cdots, \omega_\nu, t_\nu)$. 于是映射 $(w_0, \cdots, w_{m-1}) \to (w^\eta, \cdots, w^\eta_{m-1})$ 是 $\mathfrak{S}_m$ 到代数 $(\mathfrak{W}_m(\mathfrak{A}), +, \cdot)$ 内的同态，此处 $+, \cdot$ 由 (22) 所定义. 注意这个同态映 x 为 a，y 为 b，z 为 c. 还要注意当 $w_\nu \in (p)$ 时，任一个 $w=(w_\nu)$ 都在 $\mathfrak{S}_m$ 到 $\mathfrak{A}$ 内的同态核中.

现在可以证明

定理 10. $\mathfrak{W}_m(\mathfrak{A})$ 是一个交换环.

证 令 $a=(a_\nu)$，$b=(b_\nu)$，$c=(c_\nu)$ 是 $\mathfrak{W}_m(\mathfrak{A})$ 的任意三个元，刚才已经看到，有 $\mathfrak{S}_m$ 到 $\mathfrak{W}_m(\mathfrak{A})$ 内的同态使 $x=(x_\nu)\to a$，$y=(y_\nu)\to b$，$z=(z_\nu)\to c$. 故 $\mathfrak{S}_m$ 中结合律、交换律及加法与乘法的分配律给出了元素 a, b, c 间的同样规则(例如 $(ab)c=a(bc)$). 在这个同态下，$0=(0,\cdots,0)$ 和 $1=(1,0,\cdots,0)$的象是 $0=(0,\cdots,0)$ 和 $1=(\bar{1},0,\cdots,0)$，而且由关系式 $x+0=x$，$x1=x$ 给出 $\mathfrak{W}_m(\mathfrak{A})$中的关系式 $a+0=a$，$a1=a$，如果把$-x$ 在同态下的象记为 a'，则 $a+a'=0$. 因为 a, b, c 是 $\mathfrak{W}_m(\mathfrak{A})$ 中的任意元，所以这些注记表明 $\mathfrak{W}_m(\mathfrak{A})$ 是以 $0=(0,\cdots,0)$ 和 $1=(\bar{1},0,\cdots,0)$ 为零元与单位元的交换环.

我们称 $\mathfrak{W}_m(\mathfrak{A})$ 为 $\mathfrak{A}$ 上长度为m的维特向量环. 这里要指出，因为 $a\to(a)$ 是 $\mathfrak{A}$ 到 $\mathfrak{W}_m(\mathfrak{A})$ 上的同构，所以 $\mathfrak{W}_m(\mathfrak{A})$ 可以和 $\mathfrak{A}$ 本身等同.

现在设$\mathfrak{B}$是I_p上$\mathfrak{A}$的子代数，并作$\mathfrak{B}$上的维特向量环$\mathfrak{W}_m(\mathfrak{A})$. 显然，$b=(b_\nu)\to b$ 是 $\mathfrak{W}_m(\mathfrak{B})$ 到 $\mathfrak{W}_m(\mathfrak{A})$ 内的同构. 用这种方式可将 $\mathfrak{W}_m(\mathfrak{B})$ 和 $\mathfrak{W}_m(\mathfrak{A})$ 中由维特向量 $b(b_\nu \in \mathfrak{B})$ 作成的子环等同. 特别，若取 $\mathfrak{B}=I_p$，我们就得到分量在 I_p 中的向量作成的子环 $\mathfrak{W}_m(I_p)$，这个子环显然是由 p^m 个元素组成的.

我们定义 $\mathfrak{W}_m(\mathfrak{B})$ 到其自身的映射P：对 $a=(a_0, a_1, \cdots, a_{m-1})$，$a^P=(a_0^p, a_1^p, \cdots, a_{m-1}^p)$. 应注意到，如果

$$f(x_0, y_0, \cdots) \in I[x_i, y_i],$$

则 $f(a_0, b_0, \cdots)^p = f(a_0^p, b_0^p, \cdots)$. 由此以及 $\mathfrak{W}_m(\mathfrak{A})$ 的加法、

乘法定义可推出

(23) $$(a+b)^{\mathrm{P}}=a^{\mathrm{P}}+b^{\mathrm{P}};\ (ab)^{\mathrm{P}}=a^{\mathrm{P}}b^{\mathrm{P}}.$$

称 P 为 $\mathfrak{W}_m(\mathfrak{A})$ 的弗罗贝尼乌斯自同态. 我们引入 $\mathfrak{W}_m(\mathfrak{A})$ 到 $\mathfrak{W}_{m-1}(\mathfrak{A})$ 内的限制映射 $R:(a_0,\cdots,a_{m-1})^R=(a_0,\cdots,a_{m-2})$ 和 $\mathfrak{W}_{m-1}(\mathfrak{A})$ 到 $\mathfrak{W}_m(\mathfrak{A})$ 的移位映射 $V:(a_0,\cdots,a_{m-2})^V=(0,a_0,\cdots,a_{m-2})$. 立即可知 R 是一个环同态, 而且我们将看到 V 是 $\mathfrak{W}_{m-1}(\mathfrak{A})$ 的加法群到 $\mathfrak{W}_m(\mathfrak{A})$ 的加法群内的同态. 我们有

$$\begin{aligned}(a_0,\cdots,a_{m-1})^{VR}&=(0,a_0,\cdots,a_{m-2})\\&=(a_0,\cdots,a_{m-1})^{RV}.\end{aligned}$$

显然在 $\mathfrak{W}_m(\mathfrak{A})$ 中 $\mathrm{P}V=V\mathrm{P}$, $R\mathrm{P}=\mathrm{P}R$, $(VR)^m=0$ 成立.

我们证明以下重要的结论:

引理 2. 维特环中的以下关系成立:

(24) $$p1=\overbrace{1+1+1+\cdots+1}^{p}=1^{VR}.$$

(25) $$(a+b)^V=a^V+b^V.$$

(26) $$a^Vb=(ab^{VR})^V,\ a\in\mathfrak{W}_m(\mathfrak{A}),\ b\in\mathfrak{W}_{m+1}(\mathfrak{A}).$$

(27) $$pa=a^{\mathrm{P}VR}.$$

证 考虑 $\mathfrak{X}_{m-1}$, $\mathfrak{X}_m$, $\mathfrak{X}_{m+1}$ 中分量在 $I[x_i,y_i,z_k]$ 内的元素的子环 $\mathfrak{I}_{m-1}$, $\mathfrak{I}_m$, $\mathfrak{I}_{m+1}$, 和维特环一样定义它们的映射 R 和 V, 映射 P 的定义仍如前述. 考察 I 的元 $1=(1,0,\cdots,0)$, 令 $\boldsymbol{p}=p1$, $1^\varphi=(1,1,\cdots,1)$ 而且

$$\overbrace{1^\varphi\oplus1^\varphi\oplus\cdots\oplus1^\varphi}^{p}=(p,\cdots,p).$$

因此 $\boldsymbol{p}^{(\nu)}=p$, $0\leqslant\nu\leqslant m-1$. 另一方面, $1^{VR}=(0,1,0,\cdots,0)$, 由 φ 的定义给出 $(1^{VR})^{(0)}=0$, $(1^{VR})^{(\nu)}=p$, $1\leqslant\nu\leqslant m-1$. 于是有 $(1^{VR})^{(\nu)}\equiv\boldsymbol{p}^{(\nu)}(p^{\nu+1})$, $0\leqslant\nu\leqslant m-1$. 由引理 1, 这就推出 $(1^{VR})_\nu\equiv\boldsymbol{p}_\nu(p)$. 我们已经看到有一个 $\mathfrak{I}_m$ 到 $\mathfrak{W}_m(\mathfrak{A})$ 的同态使得每个 $\omega=(\omega_\nu)$ 在核内, 这里 $\omega_\nu\in(p)$. 将这些用到 1^{VR} 和 $\boldsymbol{p}$ 上, 再利用前面分量的关系, 就在 $\mathfrak{W}_m(\mathfrak{A})$ 中得到 (24). 其次, 对 $x=(x_0,\cdots,x_{m-1})\in\mathfrak{I}_m$ 和 $y=(y_0,\cdots,y_{m-1})\in\mathfrak{I}_m$, 有 $x^V=(0,x_0,\cdots,x_{m-1})$, $y^V=(0,y_0,\cdots,y_{m-1})$, 于是由 (11) 得

$$(x^V)^{(\nu)} = px_0^{p^{\nu-1}} + p^2x_1^{p^{\nu-2}} + \cdots + p^\nu x_{\nu-1},$$
$$1 \leqslant \nu \leqslant m;$$

因此

(28) $$(x^V)^{(\nu)} = px^{(\nu-1)},\ 1 \leqslant \nu \leqslant m.$$

因为 $(x+y)^{(\nu)} = x^{(\nu)} + y^{(\nu)}$, $(x^V)^{(0)} = (y^V)^{(0)} = ((x+y)^V)^{(0)} = 0$, 则 $((x+y)^V)^{(\nu)} = (x^V)^{(\nu)} + (y^V)^{(\nu)}$, $0 \leqslant \nu \leqslant m$. 因此 $(x+y)^V = x^V + y^V$ 在 $\mathfrak{I}_{m+1}$ 中成立. 如果把 $I[x_i, y_j, z_k]$ 到 $\mathfrak{A}$ 内同态: $n \to \bar{n} = n + (p)$, $x_\nu \to a_\nu$, $y_\nu \to b_\nu$, $z_\nu \to c_\nu$ 用在 $(x+y)^V$ 和 $x^V + y^V$ 的分量上, 则得到 (25) 对 $a, b \in \mathfrak{W}_m(\mathfrak{A})$ 是成立的. 为了证明 (26), 我们先证明

(29) $$(x^V y)_\nu \equiv ((xy^{PR})^V)_\nu(p),\ 0 \leqslant \nu \leqslant m.$$

如果 $x = (x_0, x_1, \cdots, x_{m-1}) \in \mathfrak{I}_m$, $y = (y_0, y_1, \cdots, y_{m+1}) \in \mathfrak{I}_{m+1}$, ($x_i, y_j$ 是未定元). 令 $x^V y = (w_0, w_1, \cdots, w_m)$, $(xy^{PR})^V = (t_0, t_1, \cdots, t_m)$. 我们必须证明 $\omega_\nu = t_\nu(p)$, $0 \leqslant \nu \leqslant m$. 由引理 1, 这等价于 $\omega^{(\nu)} \equiv t^{(\nu)}(p^{\nu+1})$. 因为 $\omega^{(0)} = 0 = t^{(0)}$, 所以该式当 $\nu = 0$ 时成立. 对于 $\nu \geqslant 1$, 由 (28), 我们有 $\omega^{(\nu)} = px^{(\nu-1)}y^{(\nu)}$, $t^{(\nu)} = px^{(\nu-1)}(y^{PR})^{(\nu-1)}$. 因为 $y^{(\nu)} = (y^P)^{(\nu-1)} + p^\nu y_\nu$, 这就给出了同余式

$$\omega^{(\nu)} = px^{(\nu-1)}y^{(\nu)} \equiv px^{(\nu-1)}(y^P)^{(\nu-1)}$$
$$\equiv px^{(\nu-1)}(y^{PR})^{(\nu-1)} \equiv t^{(\nu)}(p^{\nu+1}).$$

因此 (29) 成立, 施行一适当的到 $\mathfrak{A}$ 内的同态, 得到 (26). 如果将 R 施行于 (26) 的两边, 得到 $a^{VR}b^R = (ab^{PR})^{VR}$. 令 $a = 1$,

$$b^R = c \in \mathfrak{W}_m(\mathfrak{A}),$$

则 $1^{VR}c = c^{PVR}$. 由 (24), $1^{VR} = p1$, 这就给出 $pc = c^{PVR}$. 由于 $c = b^R$ 是取自 $\mathfrak{W}_m(\mathfrak{A})$ 的任意元, 这等价于 (27).

下面给出我们需要的 $\mathfrak{W}_m(\mathfrak{A})$ 的基本性质, 首先证明

定理 11. $\mathfrak{W}_m(\mathfrak{A})$ 是特征为 p^m 的环.

证　只要证明在 $\mathfrak{W}_m(\mathfrak{A})$ 的加法群中, 1 的阶为 p^m 即可. 已经看到 $p1 = 1^{VR} = (0, 1, 0, \cdots, 0)$, 重复使用 (27) 得到

$$p^2 1 = (0, 0, 1, 0, \cdots)$$

等等, 这表明 $p^{m-1}1 = (0, \cdots, 0, 1) \neq 0$, 但 $p^m 1 = 0$, 这就是所

要求的。

我们已经知道，如果 $\mathfrak{B}$ 是 $\mathfrak{A}$ 的子代数，那末可以把 $\mathfrak{W}_m(\mathfrak{B})$ 看作 $\mathfrak{W}_m(\mathfrak{A})$ 的子环。特别当 $\mathfrak{B}=I_P$ 时也成立，于是 $Z\equiv\mathfrak{W}_m(I_P)$ 是分量属于域 I_P 的向量集，从而 Z 中元素个数是 p^m。另一方面，定理 11 表明 $\mathfrak{W}_m(\mathfrak{A})$ 有 p^m 个形为 $k1$ (k 为整数)的不同元，而且都属于 Z。因此显然 Z 恰是 $\mathfrak{W}_m(\mathfrak{A})$ 中单位元的整数倍的集。明显地，Z 同构于模 p^m 的剩余类环 $I/(p^m)$。以下结果从一个角度研究了 $\mathfrak{W}_m(\mathfrak{A})$ 的结构。

定理 12. 映射 $a=(a_0, a_1, \cdots, a_{m-1})\to a_0$ 是 $\mathfrak{W}_m(\mathfrak{A})$ 到 $\mathfrak{A}$ 上的同态，核 $\mathfrak{N}$ 是一个幂零理想。

证 我们已知 R 是 $\mathfrak{W}_m(\mathfrak{A})$ 到 $\mathfrak{W}_{m-1}(\mathfrak{A})$ 上的同态，重复这一步骤表明 R^{m-1} 是 $\mathfrak{W}_m(\mathfrak{A})$ 到 $\mathfrak{W}_1(\mathfrak{A})=\mathfrak{A}$ 上的同态。显然 R^{m-1} 就是定理所指的映射，同态核是形为 $(0, a_0, a_1, \cdots, a_{m-2})$ 的元所成的理想 $\mathfrak{N}$。因此 $\mathfrak{N}=\mathfrak{W}_m(\mathfrak{A})^{VR}$。将 R 作用于 (26) 的两边，得到 $a^{VR}b^R=(ab^{PR})^{VR}$。因为 b^R 可以取自 $\mathfrak{W}_m(\mathfrak{A})$ 的任意元 c，这就给出 $\mathfrak{W}_m(\mathfrak{A})$ 中的关系式 $a^{VR}c=(ac^P)^{VR}$，然后

$$a^{VR}c^{VR}=(ac^{PVR})^{VR}=(a^Pc^P)^{(VR)^2}\in\mathfrak{W}_m(\mathfrak{A})^{(VR)^2}.$$

因此 $\mathfrak{N}^2=(\mathfrak{W}_n(\mathfrak{A})^{VR})^2\subseteq\mathfrak{N}^{VR}$。假设对某些 $k\geqslant 2$，有

$$\mathfrak{N}^k\subseteq\mathfrak{N}\mathfrak{N}^{(VR)^{k-2}}\subseteq\mathfrak{N}^{(VR)^{k-1}}$$

则当 $d=a^{VR}\in\mathfrak{N}$，$b\in\mathfrak{N}^k$ 时，由于 $b\in\mathfrak{N}^{(VR)^{k-1}}=\mathfrak{W}_m(\mathfrak{A})^{(VR)^k}$，故有 $b=c^{(VR)^k}$，$c\in\mathfrak{W}_m(\mathfrak{A})$。因此 $db=a^{VR}c^{(VR)^k}\in\mathfrak{N}\mathfrak{N}^{(VR)^{k-1}}$ 于是 $\mathfrak{N}^{k+1}\subseteq\mathfrak{N}\mathfrak{N}^{(VR)^{k-1}}$。但是如果 $a, c\in\mathfrak{W}_m(\mathfrak{A})$，则

$$a^{VR}c^{(VR)^k}=(a^{PVR}c^{(VR)^{k-1}})^{VR}\in(\mathfrak{N}\mathfrak{N}^{(VR)^{k-2}})^{VR}\subseteq(\mathfrak{N}^{(VR)^{k-1}})^{VR}=\mathfrak{N}^{(VR)^k},$$

所以 $\mathfrak{N}\mathfrak{N}^{(VR)^{k-1}}\subseteq\mathfrak{N}^{(VR)^k}$，于是 $\mathfrak{N}^{k+1}\subseteq\mathfrak{N}^{(VR)^k}$。这就证明了对一切 $k\geqslant 2$，有 $\mathfrak{N}^k\subseteq\mathfrak{N}^{(VR)^{k-1}}$ 成立。又因为 $\mathfrak{N}=\mathfrak{W}_m(\mathfrak{A})^{VR}$ 和

$$\mathfrak{W}_m(\mathfrak{A})^{(VR)^m}=0,$$

所以 $\mathfrak{N}^m=0$。

推论. 元 $a=(a_0, a_1, \cdots, a_{m-1})$ 是 $\mathfrak{W}_m(\mathfrak{A})$ 的单位当且仅当 a_0 是 $\mathfrak{A}$ 的单位。

证 这是定理 12 的结果。应注意的是如果 $\mathfrak{N}$ 是环 $\mathfrak{W}$ 的幂

零理想，则 $a\in\mathfrak{B}$ 是 $\mathfrak{B}$ 中的单位当且仅当陪集 $a+\mathfrak{N}$ 是 $\mathfrak{B}/\mathfrak{N}$ 的单位．我们将证明留作习题．

5. 阿贝尔 p 扩张 首先简要地考察一下特征 $p\neq 0$ 的域 Φ 的其伽罗瓦群 G 的指数为 p 的域 Φ 的交换扩张是有益的（参考本卷§2.3 习题中的第3，4两题）．在这种情况下，令 Z 是由 Φ 的元1生成的加法循环群，考虑特征标群 $\mathrm{Hom}(G,Z)$，此处 G 是限定类型的扩张 P 的伽罗瓦群．元 $\chi\in\mathrm{Hom}(G,Z)$ 是 G 到 Z 内满足

$$\chi(st)=\chi(s)+\chi(t)$$

的映射．因为 $\chi(s)\in Z\subseteq\Phi$，它也可以写成 $\chi(st)=\chi(s)^t+\chi(t)$ 的形式，因而我们得到一个与诺特方程类似的加法例子．根据定理1.20，存在 $\rho\in P$ 使 $\chi(s)=\rho^s-\rho$． 又因为 $\chi(s)\in Z$，$\chi(s)^p=\chi(s)$，所以 $(\rho^s-\rho)^p=\rho^s-\rho$．这就给出方程

$$(\rho^p-\rho)^s=\rho^p-\rho,\quad s\in G,$$

所以 $\rho^p-\rho=\alpha\in\Phi$．反之，令 ρ 是 P 中满足 $\rho^p-\rho=\alpha\in\Phi$ 的任意元，而且定义 $\chi(s)=\rho^s-\rho$，则

$$\chi(s)^p-\chi(s)=(\rho^p-\rho)^s-(\rho^p-\rho)=\alpha^s-\alpha=0,$$

所以 $\chi(s)^p=\chi(s)$．这就推出 $\chi(s)$ 在素域中，所以 $\chi(s)\in Z$．又因 $\chi(st)=\rho^{st}-\rho=(\rho^s-\rho)^t+(\rho^t-\rho)=(\rho^s-\rho)+(\rho^t-\rho)=\chi(s)+\chi(t)$；故 $\chi\in\mathrm{Hom}(G,Z)$．下面仿照库默尔理论的格式，考虑 P 中满足 $\rho^p-\rho\in\Phi$ 的元 ρ 所成子集 $S(P)$，这是加法群 $(P,+)$ 中包含 $(\Phi,+)$ 的子群，而且有 $S(P)$ 到 $\mathrm{Hom}(G,Z)$ 上的映射 $\rho\to\chi_\rho$，此处 $\chi_\rho(s)=\rho^s-\rho$．因为 Z 是加法群，所以 $\mathrm{Hom}(G,Z)$ 的合成是 $(\chi+\psi)(s)=\chi(s)+\psi(s)$．而且，如果 $\rho,\sigma\in S(P)$，则 $\chi_{\rho+\sigma}(s)=(\rho+\sigma)^s-(\rho+\sigma)=\chi_\rho(s)+\chi_\sigma(s)$；因此 $\rho\to\chi_\rho$ 是 $S(P)$ 到 $\mathrm{Hom}(G,Z)$ 上的一个同态．显然，这个同态核是 Φ，所以 $S(P)/\Phi\cong\mathrm{Hom}(G,Z)\cong G$．

下一步讨论 Φ 中形为 $\rho^p-\rho(\rho\in S(P))$ 的元所成子集 $Q(P)$，这是加法群 $(\Phi,+)$ 的子群，且包含形为 $\alpha^p-\alpha(\alpha\in\Phi)$ 的元所成子群． 容易看出 $Q(P)$ 关于后一子群的商群同构于 $S(P)/\Phi$，所以也同构于 $\mathrm{Hom}(G,Z)$ 和 G．可以证明，$(\Phi,+)$ 的任何子

群，如果含元 $\alpha^p-\alpha(\alpha\in\Phi)$ 所成子群且关于这个子群的商群有限,则这样的子群就是阿贝尔 p 扩张的群 $Q(\mathrm{P})$，此扩张的伽罗瓦群的指数 $\leqslant p$. 群 Q 给出这些扩张的概貌，就如 $N(\mathrm{P})$ 给出了库默尔扩张的概貌一样. 这里我们将不纠缠在细节问题上，而来处理任意 p 扩张的一般情形，这里的意图是从给定扩张 P 上的维特向量环 $\mathfrak{W}_m(\mathrm{P})$ 着手,此处 $m\geqslant e$，G 的指数为 p^e. 由 1 生成的 $\mathfrak{W}_m(\mathrm{P})$ 的加法群的子群 Z 是 p^m 阶循环群；因此 $\mathrm{Hom}(G, Z)$ 是 G 的特征标群. 首先，我们必须把定理 1.20 推广到维特向量环，现在着手导出这个结果.

设 P 是特征 $p\neq 0$ 的域 Φ 的有限维伽罗瓦扩域，伽罗瓦群为 G，令 $\mathfrak{W}_m(\mathrm{P})$ 是 P 上长度 $m\geqslant 1$ 的维特向量环. 已经看到，可以把 $\mathfrak{W}_m(\Phi)$ 和 $\mathfrak{W}_m(\mathrm{P})$ 中的向量 $\beta=(\beta_0, \beta_1, \cdots, \beta_{m-1})$ 所成子集等同起来，此处 $\beta_\nu\in\Phi$. 如果 $\rho=(\rho_0, \cdots, \rho_{m-1})\in\mathfrak{W}_m(\mathrm{P})$，$s\in G$，我们定义 $\rho^s=(\rho_0^s, \cdots, \rho_{m-1}^s)$. 显然 $\rho\to\rho^s$ 是 $\mathfrak{W}_m(\mathrm{P})$ 的一个自同构，这些自同构的集群同构于 G，把这个群也记作 G. 显然 $\rho^s=\rho$ 当且仅当 $\rho_\nu^s=\rho_\nu$，$0\leqslant\nu\leqslant m-1$. 因此 $\mathfrak{W}_m(\Phi)$ 可以用环 $\mathfrak{W}_m(\mathrm{P})$ 的 G 不变子环来刻划.

如果 $\rho\in\mathfrak{W}_m(\mathrm{P})$，我们定义它的迹为

$$T(\rho)=\sum_{s\in G}\rho^s.$$

显然 $T(\rho)^s=T(\rho)$，$s\in G$，于是 $T(\rho)\in\mathfrak{W}_m(\Phi)$. 如果 $\rho=(\rho_0, \rho_1, \cdots, \rho_{m-1})$，则 $T(\rho)$ 的第一个分量是 $T(\rho_0)$（迹在 Φ 上的 P 中）因为在 $\mathfrak{W}_m(\mathrm{P})$ 中求和时，第 1 个分量是相加的. 我们已知自同构 $s\in G$ 在 P 中是 P 无关的，则可推出存在 $\rho_0\in\mathrm{P}$ 使

$$T(\rho_0)\neq 0.$$

如果 ρ_0 按这个方法选取，且 $\rho=(\rho_0, \cdots)$，则

$$T(\rho)=(T(\rho_0), \cdots)$$

有非零的第一个分量. 于是从定理 12 的推论中得到 $T(\rho)$ 是 $\mathfrak{W}_m(\Phi)$ 的单位，因此证明了以下结论：

引理 1. 存在 $\rho\in\mathfrak{W}_m(\mathrm{P})$，使 $\mathfrak{W}_m(\Phi)$ 中有 $T(\rho)^{-1}$ 存在.

由此证明以下关键的上同调结果。

定理 13. 令 $s \to \mu_s$ 是 G 到 $\mathfrak{W}_m(\mathrm{P})$ 内的映射，使得 $\mu_{st} = \mu_s^t + \mu_t$，$s, t \in G$。则存在元 $\sigma \in \mathfrak{W}_m(\mathrm{P})$ 使 $\mu_s = \sigma^s - \sigma$。反之，如果 $\sigma \in \mathfrak{W}_m(\mathrm{P})$，则 $\mu_s = \sigma^s - \sigma$ 满足给定方程。

证 证明方法与定理 1.20 所处理的伽罗瓦扩域的特殊情形是一样的。我们选择 $\rho \in \mathfrak{W}_m(\mathrm{P})$ 使 $T(\rho)^{-1}$ 存在且属于 $\mathfrak{W}_m(\Phi)$，令 $\tau = T(\rho)^{-1}\left(\sum_{s \in G} \mu_s \rho^s\right)$，则

$$\tau - \tau^t = T(\rho)^{-1}\left(\sum_s (\mu_{st}\rho^{st} - \mu_s^t \rho^{st})\right)$$

$$= T(\rho)^{-1}\left(\sum_s \mu_t \rho^{st}\right)$$

$$= T(\rho)^{-1}\mu_t T(\rho) = \mu_t.$$

因此，如果取 $\sigma = -\tau$，则有 $\mu_s = \sigma^s - \sigma$，这就是所需要的。反之，如果取 $\mu_s = \sigma^s - \sigma$，这里 σ 是 P 的任意元，则有

$$\mu_s^t + \mu_t = \sigma^{st} - \sigma^t + \sigma^t - \sigma = \sigma^{st} - \sigma = \mu_{st}.$$

我们知道，弗罗贝尼乌斯映射 $\rho \to \rho^p = (\rho_0^p, \rho_1^p, \cdots \rho_m^p)$ 是环 $\mathfrak{W}_m(\mathrm{P})$ 的自同态。今在 $\mathfrak{W}_m(\mathrm{P})$ 中引入映射 $\mathfrak{P}$，定义为

$$\mathfrak{P}(\rho) = \rho^p - \rho. \tag{30}$$

显然 $\mathfrak{P}$ 是 $\mathfrak{W}_m(\mathrm{P})$ 的加法群的自同态(但不是环 $\mathfrak{W}_m(p)$ 的自同态)。$\mathfrak{P}$ 的核是满足 $\rho_\nu^p = \rho_\nu (0 \leqslant \nu \leqslant m-1)$ 的向量 $(\rho_0, \rho_1, \cdots, \rho_{m-1})$ 的集。显然，这正好是分量 ρ_i 在素域 $\Phi_0(\cong I_p)$ 的向量集。因此 $\mathfrak{P}$ 的核是维特向量 $(\rho_0, \rho_1, \cdots, \rho_{m-1})$ 的集，此处 $\rho_i \in \Phi$。已经看到(定理 11 后面)，这恰恰是单位元 1 的整数倍的集 Z，Z 在加法下是 p^m 阶循环群。

今设伽罗瓦群 G 是 p^f 阶交换群，$m \geqslant e$，p^e 是 G 的指数。令

$$S(\mathfrak{W}_m(\mathrm{P})) = \{\rho \in \mathfrak{W}_m(\mathrm{P}) \mid \mathfrak{P}(\rho) \in \mathfrak{W}_m(\Phi)\}, \tag{31}$$

则 $S(\mathfrak{W}_m(\mathrm{P}))$ 是加法群 $(\mathfrak{W}_m(p), +)$ 的、包含 $\mathfrak{W}_m(\Phi)$ 的子群。如果 $\rho \in S(\mathfrak{W}_m(\mathrm{P}))$，那末由 $\chi_\rho(s) = \rho^s - \rho$ 定义 G 的映射 χ_ρ。如果 $\mathfrak{P}(\rho) = \alpha$，则 $\chi_\rho(s)^p = \rho^{sp} - \rho^p = \rho^{ps} - \rho^p = (\rho^s +$

$\alpha)-(\rho+\alpha)$，因此 $\chi_\rho(s)^{\mathrm{P}}=\rho^s-\rho=\chi_\rho(s)$。这就推出 $\chi_\rho(s)\in Z$，又有 $\chi_\rho(st)=\rho^{st}-\rho=\rho^{st}-\rho^t+\rho^t-\rho=(\rho^s-\rho)+(\rho^t-\rho)=\chi_\rho(s)+\chi_\rho(t)$。因此 $\chi_\rho\in\mathrm{Hom}(G,Z)$，然后令 $\rho,\sigma\in S(\mathfrak{W}_m(\mathrm{P}))$，则 $\rho+\sigma\in S(\mathfrak{W}_m(\mathrm{P}))$，且 $\chi_{\rho+\sigma}(s)=(\rho+\sigma)^s-(\rho+\sigma)=(\rho^s-\rho)+(\sigma^s-\sigma)=\chi_\rho(s)+\chi_\sigma(s)$。这就证明了映射 $\rho\to\chi_\rho$ 是 $S(\mathfrak{W}_m(\mathrm{P}))$ 到 $\mathrm{Hom}(G,Z)$ 内的同态。如果对一切 $s\in G$ 有 $\chi_\rho(s)=0$，则 $\rho^s=\rho$，$s\in G$。这就推出 $\rho\in\mathfrak{W}_m(\Phi)$。因此

$$\rho\to\chi_\rho$$

的核是 $\mathfrak{W}_m(\Phi)$，最后，这个同态是满射。令 $\chi\in\mathrm{Hom}(G,Z)$，则 $\chi(st)=\chi(s)+\chi(t)$。因为 $\chi(s)\in Z$，故也有 $\chi(st)=\chi(s)^t+\chi(t)$。于是由定理 13，存在 $\rho\in\mathfrak{W}_m(\mathrm{P})$ 使 $\chi(s)=\rho^s-\rho$。因为 $\chi(s)\in Z$，$\chi(s)^p=\chi(s)$，这就给出 $(\rho^{\mathrm{P}}-\rho)^s=\rho^p-\rho$。因此 $\mathfrak{P}(\rho)=\rho^{\mathrm{P}}-\rho\in\mathfrak{W}_m(\Phi)$，于是 $\rho\in S(\mathfrak{W}_m(\mathrm{P}))$。现在我们看到 $S(\mathfrak{W}_m(\mathrm{P}))$ 到 $\mathrm{Hom}(G,Z)$ 的映射 $\rho\to\chi_\rho$ 是满射。因为核是 $\mathfrak{W}_m(\Phi)$，我们有 $S(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{W}_m(\Phi)\cong\mathrm{Hom}(G,Z)\cong G$，这就证明了和定理 7 完全类似的下述定理的前两个命题：

定理 14. 令 Φ 是特征 $p\neq0$ 的域，P/Φ 是一个阿贝尔 p 扩张，其伽罗瓦群 G 的指数为 p^e，$\mathfrak{W}_m(\mathrm{P})$ 是 P 上长度为 m 的维特向量环 $(m\geqslant e)$。$S(\mathfrak{W}_m(\mathrm{P}))$ 如 (31) 所定义，则存在加法群的正合序列

$$0\to\mathfrak{W}_m(\Phi)\to S(\mathfrak{W}_m(\mathrm{P}))\to\mathrm{Hom}(G,Z)\to0,$$

其中 $\mathfrak{W}_m(\Phi)$ 的同态是包含映射，$S(\mathfrak{W}_m(\mathrm{P}))$ 到 $\mathrm{Hom}(G,Z)$ 内的同态是 $\rho\to\chi_\rho$，$\chi_\rho(s)=\rho^s-\rho$。商群 $S(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{W}_m(\Phi)$ 是有限的，且同构于 G。域 P/Φ 由向量 $\rho\in S(\mathfrak{W}_m(\mathrm{P}))$ 的分量生成，而且

$$\mathrm{P}=\Phi(\rho_0^{(1)},\cdots,\rho_{m-1}^{(1)};\rho_0^{(2)},\cdots,\rho_{m-1}^{(2)};\cdots;\rho_0^{(r)},\cdots,\rho_{m-1}^{(r)})$$

当且仅当陪集 $\rho^{(i)}+\mathfrak{W}_m(\Phi)$ 生成 $S(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{W}_m(\Phi)$，其中

$$\rho^{(i)}=(\rho_0^{(i)},\cdots,\rho_{m-1}^{(i)}).$$

最后一个命题的证明和定理 7 的相应命题一样，留给读者详细验证。

下面按照库默尔理论的处理方式引入集

$$(32)\qquad Q(\mathfrak{W}_m(\mathrm{P}))=\{\mathfrak{P}(\rho)\mid\rho\in S(\mathfrak{W}_m(\mathrm{P}))\}$$
$$=\mathfrak{W}_m(\Phi)\cap\mathfrak{P}(\mathfrak{W}_m(\mathrm{P})).$$

这是加法群 $(\mathfrak{W}_m(\Phi),+)$ 的子群，而且包含向量 $\mathfrak{P}(\alpha)$ $(\alpha\in\mathfrak{W}_m(\Phi))$ 所成的子群 $\mathfrak{P}(\mathfrak{W}_m(\Phi))$. 考虑 $S(\mathfrak{W}_m(\mathrm{P}))$ 到

$$Q(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{P}(\mathfrak{W}_m(\Phi))$$

上的同态

$$\rho\to\mathfrak{P}(\rho)+\mathfrak{P}(\mathfrak{W}_m(\Phi)).$$

一个元 ρ 属于这一同态核当且仅当 $\mathfrak{P}(\rho)=\mathfrak{P}(\alpha)$, $\alpha\in\mathfrak{W}_m(\Phi)$. 这又等价于 $\mathfrak{P}(\rho-\alpha)=0$, 即 $\rho-\alpha\in Z$. 所以同态核显然是 $\mathfrak{W}_m(\Phi)$, 且有同构关系

$$(33)\qquad Q(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{P}(\mathfrak{W}_m(\Phi))\cong S(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{W}_m(\Phi).$$

由此推出 $Q(\mathfrak{W}_m(\mathrm{P}))/\mathfrak{P}(\mathfrak{W}_m(\Phi))$ 是有限群且同构于 $\mathrm{Hom}(G,Z)$ 和 G. 下面希望证明，如果 Q 是 $\mathfrak{W}_m(\Phi)$ 的任意子群而且 Q 含有子群 $\mathfrak{P}(\mathfrak{W}_m(\Phi))$, 其指数有限，则对 Φ 上的阿贝尔 p 扩张 P 有 $Q=Q(\mathfrak{W}_m(\mathrm{P}))$. 为此，我们需要

引理 2. 令 $\beta=(\beta_0,\beta_1,\cdots,\beta_{m-1})\in\mathfrak{W}_m(\Phi)$, 则存在 Φ 的有限维可分扩域 P, 使 $\mathrm{P}=\Phi(\rho)\equiv\Phi(\rho_0,\rho_1,\cdots,\rho_{m-1})$, 而且 $\mathfrak{W}_m(\mathrm{P})$ 的元 $\rho=(\rho_0,\rho_1,\cdots,\rho_{m-1})$ 满足 $\mathfrak{P}(\rho)=\beta$.

证　当 $m=1$ 时，就是要构造一个由方程 $x^p-x=\beta(\beta\in\Phi)$ 的根 ρ 生成的可分扩张 $\mathrm{P}=\Phi(\rho)$. 因为导数 $(x^p-x-\beta)'=-1$, 则方程有不同根，因此任何由这个方程的一个根生成的域都满足条件. 现在假设已经构造出可分扩张 $E=\Phi(\rho_0,\cdots,\rho_{m-2})$, 使 $\mathfrak{W}_{m-2}(E)$ 的向量 $\sigma=(\rho_0,\cdots,\rho_{m-2})$ 满足 $\mathfrak{P}(\sigma)=(\beta_0,\cdots,\beta_{m-2})$. 考虑多项式环 $E[x]$ 和维特环 $\mathfrak{W}_m(E[x])$, 在这个环中取向量 $y=(\rho_0,\cdots,\rho_{m-2},x)$, 作

$$\mathfrak{P}(y)=(\rho_0^p,\cdots,\rho_{m-2}^p,x^p)-(\rho_0,\cdots,\rho_{m-2},x),$$

则 $\mathfrak{P}(y)=(\beta_0,\beta_1,\cdots,\beta_{m-2},f(x))$, $f(x)\in E[x]$. 因此 $(\beta_0,\beta_1,\cdots,\beta_{m-2},f(x))+(\rho_0,\cdots,\rho_{m-2},x)=(\rho_0^p,\cdots,\rho_{m-2}^p,x^p)$, 由公式 (15) 知,

(34) $$x^p = f(x) + x + \gamma$$

此处 $\gamma \in E$. 所以 $f(x) = x^p - x - \gamma$. 利用导数判断表明

$$f(x) = \beta_{m-1}$$

有不同的根. 如果 $\mathrm{P} = E(\rho_{m-1})$, 此处 $f(\rho_{m-1}) = \beta_{m-1}$, 则 P 是 E 上的可分扩张, 于是 $\mathrm{P} = \Phi(\rho_0, \cdots, \rho_{m-1})$, 在 Φ 上是可分的. 由上面给出的公式, 显然 $\rho = (\rho_0, \cdots, \rho_{m-1})$ 是 $\mathfrak{W}_m(\mathrm{P})$ 的元, 且 $\mathfrak{P}(\rho) = \beta$.

现在可以证明

定理 15. 令 Q 是 $(\mathfrak{W}_m(\Phi), +)$ 的包含 $\mathfrak{P}(\mathfrak{W}_m(\Phi))$ 的子群, 而且 $Q/\mathfrak{P}(\mathfrak{W}_m(\Phi))$ 是有限的, 则存在 Φ 的阿贝尔 p 扩张 P, 使其伽罗瓦群的指数为 p^e, $e \leqslant m$, 而且 $Q(\mathfrak{W}_m(\mathrm{P})) = Q$.

证 令 $\beta^{(1)}, \beta^{(2)}, \cdots, \beta^{(r)}$ 是 Q 的元, 使陪集 $\beta^{(i)} + \mathfrak{P}(\mathfrak{W}_m(\Phi))$ 生成 $Q/\mathfrak{P}(\mathfrak{W}_m(\Phi))$. 由引理 2, 可以构造一个 Φ 上的有限维可分扩张域 P, 而 P 由满足 $\mathfrak{P}(\rho_0^{(i)}, \cdots, \rho_{m-1}^{(i)}) = (\beta_0^{(i)}, \cdots, \beta_{m-1}^{(i)}) \in \mathfrak{W}_m(\mathrm{P})$ 的元 $\rho_v^{(i)}(1 \leqslant i \leqslant r,\ 0 \leqslant v \leqslant m-1)$ 生成. 设 Ω 是 Φ 上包含 P 的有限维伽罗瓦扩张域, 作 $\mathfrak{W}_m(\Omega)$, 和前面一样, Ω/Φ 的伽罗瓦群 G 作用在 $\mathfrak{W}_m(\Omega)$ 上. 如果 $s \in G$, $\rho^{(i)} = (\rho_0^{(i)}, \cdots, \rho_{m-1}^{(i)})$, 则 $\mathfrak{P}(\rho^{(i)}) = \beta^{(i)}$ 给出 $\mathfrak{P}(\rho^{(i)s}) = \beta^{(i)}$, 因此

$$\mathfrak{P}(\rho^{(i)s} - \rho^{(i)}) = 0,$$

所以 $\rho^{(i)s} - \rho^{(i)} \in Z \subseteq \mathfrak{W}_m(\Phi)$. 这就推出 $\mathrm{P}^s \subseteq \mathrm{P}$, $s \in G$, 于是 P 是 Φ 上的伽罗瓦扩张. 因而我们可以取 $\Omega = \mathrm{P}$. 如果 s, t 是在 Φ 上 P 的伽罗瓦群 G 中, 则 $\rho^{(i)s} = \rho^{(i)} + \gamma^{(i)}$, 而且 $\rho^{(i)t} = \rho^{(i)} + \delta^{(i)}$, 此处 $\gamma^{(i)}$, $\delta^{(i)} \in \mathfrak{W}_m(\Phi)$. 因此 $\rho^{(i)st} = \rho^{(i)} + \gamma^{(i)} + \delta^{(i)} = \rho^{(i)ts}$, 由此推出 G 是交换的. 又因为 $\rho^{(i)s^k} = \rho^{(i)} + k\gamma^{(i)}$, 且由于 $\mathfrak{W}_m(\mathrm{P})$ 的特征为 p^m, 故 $\rho^{(i)s^{p^m}} = \rho^{(i)}$. 这就证明了 $s^{p^m} = 1$, 所以 G 是指数为 p^e 的 p^f 阶群, $e \leqslant m$. 令 χ_i 是由 $\rho^{(i)}$: $\chi_i(s) \equiv \rho^{(i)s} - \rho^{(i)}$ 决定的 G 的特征标. 那末显然由 $\chi_i(s) = 1 (1 \leqslant i \leqslant r)$ 推出 $s = 1$, 于是 χ_i 生成特征标群 $\mathrm{Hom}(G, Z)$. 因此, 如果 ρ 是使得 $\mathfrak{P}(\rho) \in \mathfrak{W}_m(\Phi)$ 的 $\mathfrak{W}_m(\mathrm{P})$ 的任意元, 则 $\chi_\rho = \Pi \chi_i^{m_i}$, 由此推出

$$\rho = \Sigma m_i \rho^{(i)} + \beta,\ \beta \in \mathfrak{W}_m(\Phi),$$

m_i 是整数，于是

$$\mathfrak{P}(\rho) = \Sigma m_i \beta^{(i)} + \mathfrak{P}(\beta) \in Q.$$

因为 ρ 是 $S(\mathfrak{W}_m(\mathrm{P}))$ 的任意元．这就证明了 $Q(\mathfrak{W}_m(\mathrm{P})) \subseteq Q$．其逆命题是显然的．证毕．

现在得到的结果相当于库默尔扩张的主要结果．由此可得出：指数为 $p^e (e \leqslant m)$ 的伽罗瓦群的两个阿贝尔 p 扩张 P_1/Φ，P_2/Φ 同构当且仅当 $Q(\mathfrak{W}_m(\mathrm{P}_1)) = Q(\mathfrak{W}_m(\mathrm{P}_2))$（下面习题中的第2题）．某一特定的域 Ω/Φ 的各子域 P/Φ 间的次序和加法群 $(\mathfrak{W}(\Phi), +)$ 的各子群 $Q(\mathfrak{W}_m(\mathrm{P}))$ 间的次序保持对应关系（下面习题中的第1题）．现在考虑循环 p 扩张的特殊情况：由我们的结果可立即得到 Φ 上 p 维循环扩张形如 $\Phi(\rho)$，其中 $\rho^p - \rho = \beta \in \Phi$，$\beta \notin \mathfrak{P}(\Phi)$，即 $\beta \neq \alpha^p - \alpha$，$\alpha \in \Phi$．现在证明，如果 Φ 上存在这样的扩张，这等价于条件 $\Phi \neq \mathfrak{P}(\Phi)$，则存在 Φ 上 p^m 维循环扩张（$m = 1, 2, \cdots$），这是由下述引理得到的．

引理 3. 如果 $\beta_0, \cdots, \beta_{m-1} \in \Phi$，则 $\beta_0 \in \mathfrak{P}(\Phi)$ 当且仅当

$$\beta = (\beta_0, \beta_1, \cdots, \beta_{m-1})$$

满足 $p^{m-1}\beta \in \mathfrak{P}(\mathfrak{W}_m(\Phi))$．

证　由(27)，$p^{m-1}\beta = (0, \cdots, 0, \beta_0^{p^{m-1}})$，我们有

$$\begin{aligned}(0, \cdots, 0, \beta_0) - (0, \cdots, 0, \beta_0^{p^{m-1}}) &= (0, \cdots, 0, \beta_0) \\ &- (0, \cdots, 0, \beta_0^p) + (0, \cdots, 0, \beta_0^p) \\ &- (0, \cdots, 0, \beta_0^{p^2}) + \cdots + (0, \cdots, 0, \beta_0^{p^{m-2}}) \\ &- (0, \cdots, 0, \beta_0^{p^{m-1}}) \in \mathfrak{P}(\mathfrak{W}_m(\Phi)).\end{aligned}$$

因此 $p^{m-1}\beta = (0, \cdots, 0, \beta_0^{p^{m-1}}) \in \mathfrak{P}(\mathfrak{W}_m(\Phi))$ 当且仅当 $(0, \cdots, 0, \beta_0) \in \mathfrak{P}(\mathfrak{W}_m(\Phi))$．假若后一条件成立，即

$$(0, \cdots, 0, \beta_0) = \alpha^p - \alpha,$$

此处 $\alpha = (\alpha_0, \alpha_1, \cdots, \alpha_{m-1})$，则 $\alpha^{pR} - \alpha^R = (0, \cdots, 0, \beta_0)^R = 0$，于是 $\alpha^{Rp} = \alpha^R$，如果 $\gamma = (\alpha_0, \alpha_1, \cdots, \alpha_{m-2}, 0)$，则 $\gamma^p = \gamma$，所以 $\delta = \alpha - \gamma$ 满足 $\delta^p - \delta = (0, \cdots, 0, \beta_0)$．但是 $\delta = (0, \cdots, 0, \delta_{m-1})$，这就推出 $\delta_{m-1}^p - \delta_{m-1} = \beta_0$，所以 $\beta_0 \in \mathfrak{P}(\Phi)$．反之，若 $\beta_0 \in \mathfrak{P}(\Phi)$，即 $\beta_0 = \alpha_{m-1}^p - \alpha_{m-1}$，则 $\alpha^p - \alpha = (0, \cdots, 0,$

β_0)，此处 $\alpha=(0,\cdots,0,\alpha_{m-1})$.

现在可以证明

定理 16. 令 Φ 是特征为 $p\neq 0$ 的域，则存在 Φ 上 $p^m(m=1,2,3,\cdots)$ 维循环扩张当且仅当存在 p 维循环扩张. 与此相应的条件是 $\Phi\neq\mathfrak{P}(\Phi)$.

证 我们已经看到存在 Φ 上 p 维循环扩张当且仅当

$$\Phi\neq\mathfrak{P}(\Phi).$$

假设该条件成立，选择 $\beta_0\in\Phi$, 但 $\beta_0\notin\mathfrak{P}(\Phi)$. 令 $\beta=(\beta_0,\beta_1,\cdots,\beta_{m-1})$, $\beta_i(i>0)$ 是 Φ 的任意元. 我们已经证明 $p^{m-1}\beta\notin\mathfrak{P}(\Phi)$, 这就推出 $\mathfrak{W}_m(\Phi)$ 的子群 Q 由 β 生成，且 $Q/\mathfrak{P}(\mathfrak{W}_m(\Phi))$ 是 p^m 阶循环群. 由定理 15，对一个阿贝尔 p 扩张 P，有 $Q=Q(\mathrm{P})$. 但已知 P/Φ 的伽罗瓦群同构于 $Q/\mathfrak{P}(\mathfrak{W}_m(\Phi))$，所以这是 Φ 上 p^m 维循环扩张.

习 题 25

1. 令 P_1, P_2 是含于同一域 Ω 内的 Φ 的两个阿贝尔 p 扩张. 证明 $\mathrm{P}_1\supseteq\mathrm{P}_2$ 当且仅当 $Q(\mathfrak{W}_m(\mathrm{P}_1))\supseteq Q(\mathfrak{W}_m(\mathrm{P}_2))$, 此处 $m\geqslant e_1$, p^{e_1} 是 P_1/Φ 的伽罗瓦群的指数.

2. 令 P_i 与 m 如第 1 题，但不假定 P_i 含于同一 Ω 内，证明 Φ 上的 P_1 与 P_2 同构当且仅当 $Q(\mathfrak{W}_m(\mathrm{P}_1))=Q(\mathfrak{W}_m(\mathrm{P}_2))$.

3. 证明：如果 β 是 $\mathfrak{W}_m(\Phi)$ 的元使 $p^{m-1}\beta\in\mathfrak{P}(\mathfrak{W}_m(\Phi))$ 成立，则存在

$$\gamma\in\mathfrak{W}_m(\Phi),$$

使 $p\gamma=\beta$. 由此证明特征为 p 的 Φ 上任何 p^{m-1} 维循环扩张能嵌入 Φ 上 p^m 维循环扩张中.

第 四 章

域的构造理论

本章我们要分析一个域Φ的任意扩张域.在第一章中,已经研究了有限维扩张域，还对代数扩张作了部分的研究．本章主要涉及无限维扩张,而且仍从代数扩张开始．我们将定义代数闭域,证明任何域的代数闭包的存在性．并推广经典的伽罗瓦理论，把它应用到无限维正规扩张和可分扩张．然后将考虑任意扩张域，我们将证明这些扩张可由两步构成：第一步作一个纯超越扩张，第二步是在这个超越扩张上作一个代数扩张．生成一个域的这种方式的不变量是超越次数，即超越基的基数．我们将得到一个超越基存在的各条件，使该扩张是这组超越基所决定的纯超越扩张上的可分代数扩张．还要推广代数可分性的概念．以给出扩张域的可分性定义．在讨论中，导数的概念起着重要的作用．而且这个概念可用于推导指数为 1 的有限维纯不可分扩张的伽罗瓦理论．还要扼要说一下高阶导数的概念，它对指数大于 1 的纯不可分扩张有用．本章最后考虑非代数扩张的张量积，并用来研究域的自由合成．

1. 代数闭域 “代数基本定理”是说：系数在复数域上的每一代数方程 $f(x)=0$ 在该域中有根．具有这种性质的任何域称为代数闭域,如果Φ是一个代数闭域,则每一正次数的多项式$f(x)\in\Phi[x]$ 在 $\Phi[x]$ 中有一次因式 $x-\rho$. 于是每个 $f(x)$ 都能写成 $\Phi[x]$ 中一次因式的乘积．显然逆命题也成立：如果 $\Phi[x]$ 的每一正次数多项式是 $\Phi[x]$ 中一次因式之积,则Φ是代数封闭的.我们知道,所谓域Φ在扩张域P中是代数封闭的,指的是P在Φ上的代数元只能是Φ的元(§ 1.9)．现在我们指出，域Φ是代数封闭的

当且仅当它在每一扩张域中是代数封闭的. 令Φ是代数封闭的, P是一个扩张域, $\rho\in$ P是Φ上的代数元, $f(x)$是它的最小多项式. 因为$f(x)$不可约, Φ是代数封闭的, 所以$f(x)$是一次的, 因此$\rho\in\Phi$. 反之, 假设Φ在每一扩张域中是代数封闭的, 且$f(x)$是$\Phi[x]$中正次数不可约多项式, 则能作出扩张域 $P=\Phi[x]/(f(x))$. 其维数等于$f(x)$的次数. 因为P是Φ的代数扩张域, 而Φ在P中是代数封闭的, 则 $P=\Phi$. 因此 $\deg f(x)=1$. 这就表明, $\Phi[x]$中正次数不可约多项式只能是一次因式. 这就表明Φ是代数封闭的.

令Φ是任意域, P是Φ的代数闭扩张域, A/Φ 是 P/Φ 的代数元所成的子域. 若$f(x)\in A[x]$, 则在 $P[x]$ 中有

$$f(x)=\Pi(x-\rho_i),$$

显然ρ_i是A上的代数元素. 因为A在P中是代数封闭的(§ 1.9), 则 $\rho_i\in A$. 所以 $A[x]$ 中每一正次数的多项式是 $A[x]$ 的一次因式之积, 这就推出A是代数封闭的. 因此, 对于给定域Φ, 如果存在含Φ的代数闭域, 则就存在Φ的代数封闭的代数扩张域. 由此引出定义: 扩张域 A/Φ 叫作Φ的**代数闭包**, 假如 1) A是Φ的代数扩张域, 2) A是代数封闭的. 我们着手证明任何域Φ的代数闭包之存在性及在同构意义下的唯一性.

若Φ可数时, 有一个颇为直截了当的方法来构造Φ的代数闭包. 在此情况下, 我们容易列出正次数首项系数为1的多项式: $f_1(x)$, $f_2(x)$, $f_3(x)$, $\cdots$. 从 $\Phi_0=\Phi$ 开始, 在 Φ_{i-1} 上归纳地构造$f_i(x)$的分裂域Φ_i. 有一种简单的方法可以清楚地给出所有Φ_i的并 $A=\bigcup\Phi_i$ 的概念, 这样一来我们就可以按以下方法立即证明A是Φ的代数闭包: 首先, 显然 A/Φ 是代数的. 令P是A的代数扩张且 $\rho\in P$, 因为ρ是A上的代数元, 而A是Φ上的代数扩张, 故ρ是Φ上的代数元, 因此ρ在Φ上的最小多项式 $f(x)$ 是多项式 $f_i(x)$ 中的一个, 不妨设 $f(x)=f_n(x)$, 因为 Φ_n 包含$f(x)$的所有根, 故 $\rho\in\Phi_n\subseteq A$. 这就证明了A是代数封闭的.

借助于超限归纳法, 可将上述方法用于一般情形. 但我们宁

愿给出另一种卓伦(Zorn)[1]引理之上的构造方法。我们尚需下列结论

引理. 如果 A 是无限域 Φ 的代数扩张，则基数 $|A|=|\Phi|$.

证 令 Σ 是 $\Phi[x]$ 中正次数首项系数为 1 的多项式所成的子集，$\Sigma^{(n)}$ 是 Σ 中次数为 $n+1=1,2,3,\cdots$ 的多项式所成的子集。$\Sigma^{(n)}$ 的元形为 $x^{n+1}+\alpha_1x^n+\alpha_2x^{n-1}+\cdots+\alpha_n$, $\alpha_i\in\Phi$. 所以 $\Sigma^{(n)}$ 与 n 重积集 $\Phi\times\Phi\times\cdots\times\Phi$ 有相同的基数. 因为 Φ 是无限的，$|\Sigma^{(n)}|=|\Phi\times\Phi\times\cdots\times\Phi|=|\Phi|$，则

$$|\Sigma|=|\cup\Sigma^{(n)}|=|\Phi|^{2)}.$$

现将每个 $f(x)\in\Sigma$ 映射到有限集 R_f（可能是空集）内，而 R_f 是 $f(x)$ 在 A 中的根的集. 因为 A 的每一元是代数元，所以

$$\bigcup_{f\in\Sigma}R_f=A.$$

又因为每一 R_f 有限，故 A 的这些子集族 $\{R_f\}$ 的基数等于 $|A|$，从而 $|A|=|\{R_f\}|\leqslant|\Sigma|=|\Phi|$. 由此即推出 $|A|=|\Phi|$.

我们现在可以证明

定理 1. 任何域都有一个代数闭包.

证 设 Φ 是一个给定的域，在以下意义下可以把 Φ 嵌入一个比它大得多的集 Ω 中：如果 Φ 是有限的，则 Ω 是非可数的；如果 Φ 是无限的，则 $|\Omega|>|\Phi|$. 现在由 Ω 中含 Φ 的子集 E 出发作 Φ 的扩张域. 更明确地说，考虑一切三元系 $(E,+,\cdot)$ 的集族 Γ，其中 E 是 Ω 的含 Φ 的子集，$+$ 与 $\cdot$ 是 E 的二元合成，并且以这些合成作为加法与乘法的 E 是 Φ 的一个代数扩张域. 如果 E_2 是 E_1 的扩张域，则用 $(E_1,+_1,\cdot_1)<(E_2,+_2,\cdot_2)$，来定义 Γ 的偏序. Γ 的任何线性序子集族 $(E_\alpha,+_\alpha,\cdot_\alpha)$ 必有一上界，其基础集是 $E_\circ$

1) 卓伦(Zorn)引理在卷 2 的一些地方已经用过，此引理或“最大原理”的适当论述可见克利(Kelley)著《一般拓扑学》(General Topology) 1955 年版 p.33. ——著者注.

2) 基数的性质可参考西尔品斯基 (Sierpinski)《超越数教程》(Leçons Sur les Nombers Transfinis) 巴黎，1928 年版. ——著者注.

的并，而其加法与乘法按常规定义。这样就可以应用卓伦引理并给出集族Γ的一个极大元（A，$+$，$\cdot$）. 则A是代数封闭的，否则，A有一个真代数扩张B. 由引理，如果Φ无限，则

$$|B| = |A| = |\Phi|;$$

如果Φ有限，则$|A|$和$|B|$可数. 在这两种情况下均有

$$|B| < |\Omega|.$$

由此推出存在一个B到Ω内的1—1映射，这个映射在A上是恒等映射. 用这个映射把Ω中的象B'改为A上同构于E的域，于是（B'，$+$，$\cdot$）在集族Γ内，其加法$+$与乘法$\cdot$是由B的$+$与$\cdot$照搬过来的. 而且$B'\supset A$，这与（A，$+$，$\cdot$）的极大性矛盾，所以A是代数封闭的. 因为A在Φ上是代数的，所以A是Φ的代数闭包.

下面推广分裂域的概念，并证明一个结果，作为这一结果的特殊情形，就可得到代数闭包的唯一性. 考虑系数在Φ中的正次数多项式的集Ω，我们称扩张域P/Φ是Ω的**分裂域**，假如. (1) Ω中每一多项式都是$\mathrm{P}[x]$中线性因式之积；(2) P/Φ没有满足(1)的真子域. 设A是Φ的代数闭包，P是由一切多项式$f\in\Omega$的根生成的A/Φ的子域. 显然P是集Ω在Φ上的分裂域，A本身也是$\Phi[x]$中正次数多项式的完全集在Φ上的分裂域. 下面定理是多项式分裂域定理(定理1.8)的推广，而Φ的任意两个代数闭包在Φ上同构这一性质显然是下述定理的一个推论.

定理2. 令$\alpha\to\bar{\alpha}$是域Φ到域$\bar{\Phi}$上的同构，Ω是$\Phi[x]$中正次数多项式的集. $\bar{\Omega}$是$\Phi[x]$到$\bar{\Phi}[x]$上同构$g(x)\to\bar{g}(x)$下$f\in\Omega$的象集. P/Φ是Ω的分裂域，$\bar{\mathrm{P}}/\bar{\Phi}$是$\bar{\Omega}$的分裂域，则$\Phi$到$\bar{\Phi}$上的同构可以扩张为$\mathrm{P}$到$\bar{\mathrm{P}}$上的同构.

证　考虑P/Φ的子域到$\bar{\mathrm{P}}/\bar{\Phi}$的子域上的那些同构$s$的集族$\Delta$，这些同构$s$与$\Phi$到$\bar{\Phi}$上的同构$\alpha\to\bar{\alpha}$相一致. 我们可如下将$\Delta=\{s\}$偏序化：如果$s_2$是$s_1$的扩张，则$s_1<s_2$. 显然$\Delta$是可归纳的，也就是说，$\Delta$的每一线性有序子集必有一上界. 因此可以引用卓伦引理得到一个极大元$t\in\Delta$，则t是将$\alpha\to\bar{\alpha}$延拓而

得的 P 到 $\bar{\text{P}}$ 上的同构．否则，ε 的定义域是 P/Φ 的真子域 E，因为 P/Φ 是 Ω 的分裂域，且 $E\subset\text{P}$，所以存在多项式 $f(x)\in\Omega$，它的根不全在 E 中．因此如果 $\rho_1, \rho_2, \cdots, \rho_n$ 是在 P 中的根，则 $E(\rho_1, \rho_2, \cdots, \rho_n)\supset E$，而且显然 $E(\rho_1, \rho_2, \cdots, \rho_n)$ 是 $f(x)$ 在 E 上的分裂域．另一方面，$\bar{E} = E^{\varepsilon}$ 能嵌入 $\bar{\text{P}}$ 的一个子域、即 $\bar{f}(x)\in\bar{\Omega}$ 在 $\bar{E}$ 上的分裂域中．利用单一多项式的定理，可把 ε 延拓为 $E(\rho_1, \rho_2, \cdots, \rho_n)$ 到 $\bar{f}(x)$ 在 $\bar{E}$ 上的分裂域上的同构．这和 ε 的极大性矛盾．所以 $E = \text{P}$．显然象 P^{ε} 是 $\bar{\Omega}$ 在 $\bar{\Phi}$ 上的一个分裂域。所以 $\text{P}^{\varepsilon} = \bar{\text{P}}$．证毕．

在这一结果中，取 $\bar{\Phi} = \Phi$，$\bar{a} = \alpha$，则多项式集在 Φ 上的任何两个分裂域在 Φ 上同构．特别有

推论． 域 Φ 的任何两个代数闭包在 Φ 上同构．

令 A 是域 Φ 的代数闭包，A/Φ 有两个子域是特别有趣的．一是 Φ 上可分元所成的子域 Σ，它也可定义为 $\Phi[x]$ 中可分多项式集在 Φ 上的分裂域，我们可称 Σ 为 Φ 的可分代数闭包．其次，令 Φ 的特征 $p\neq 0$，$\Phi^{p^{-\infty}}$ 是 A 在 Φ 上纯不可分元所成子域，由 § 1.9 的引理 2，可知 A 的这些元是形为 $x^{p^e} - \alpha = 0(\alpha\in\Phi)$ 的方程的根．如果 Φ 的特征 $p\neq 0$，则称 $\Phi^{p^{-\infty}}$ 为 Φ 的完全闭包；如果 Φ 的特征为 0，则 Φ 的完全闭包是 Φ 本身．当 $p\neq 0$ 时，$\Phi^{p^{-\infty}}$ 的每一元都可写成 p 次幂，因此映射 $\alpha\to\alpha^p$ 是 $\Phi^{p^{-\infty}}$ 的一个自同构，而且 $\Phi^{p^{-\infty}}$ 是 A 在 Φ 上具有以下性质的最小子域：其所有元均是该子域的元的 p 次幂．

假如 Φ 的每一代数扩张都是可分的，则称 Φ 是完全的．刚才所定义的任何域的完全闭包是一个完全域；因为我们有以下的

定理 3． 特征为 0 的域是完全的．而特征 $p\neq 0$ 的域 Φ 是完全的当且仅当 $\Phi = \Phi^p$．即 Φ 的每一元都是 Φ 的一个 p 次幂．

证　因为不可分多项式仅当 $p\neq 0$ 时才存在，故第一个命题是显然的．令 Φ 的特征 $p\neq 0$，假设 $\Phi^p\subset\Phi$，若 $\alpha\in\Phi$，但却不是 Φ 中元的 p 次幂，则 $x^p - \alpha$ 在 $\Phi[x]$ 中不可约且不可分（§ 1.6 引理）．所以 $\text{P} = \Phi[x]/(x^p - \alpha)$ 是 Φ 的(不同于 Φ 的)不可分扩

张，于是Φ不是完全的．反之，假若 $\Phi^p=\Phi$，$f(x)$ 是 $\Phi[x]$ 中使 $f'(x)=0$ 的多项式，则能写成 $f(x)=g(x^p)$，此处

$$g(x)=x^m+\beta_1x^{m-1}+\cdots+\beta_m.$$

令 $\gamma_i^p=\beta_i$，$i=1,2,3,\cdots,m$．且 $h(x)=x^m+\gamma_1x^{m-1}+\cdots+\gamma_m$．则有 $f(x)=g(x^p)=h(x)^p$．这样，$\Phi[x]$ 中每一导数为零的多项式是一个 p 次幂．于是，$\Phi[x]$ 中不存在正次数的不可约不可分多项式，所以Φ没有真的不可分代数扩张域．

如果Φ是特征为p的有限域，则Φ到Φ^p的同构 $\alpha\to\alpha^p$ 必然是一个自同构．由定理3，每一有限域是完全域．

习　题　26

1．设E是Φ的代数扩张，A是Φ的代数闭包，证明 E/Φ 同构于 A/Φ 的一个子域．(提示：考虑E的代数闭包，并注意这是Φ的一个代数闭包．)

2．证明，如果Φ的特征 $p\neq0$，ξ 是Φ上的超越元，则 $\Phi(\xi)$ 不是完全的．

3．证明，完全域的任一代数扩张是完全的．

4．设Φ是一个域，Φ^* 是它的完全闭包．证明 $\Phi^*=\Phi$ 或者 $[\Phi^*:\Phi]$ 无限．

5．证明，任何代数闭域都是无限的．

一个域如果是其素域的代数扩张，则称这个域是**绝对代数的**．有限域就是这方面的例子．我们知道，对每一素数p与整数n，在同构意义下有且仅有一个基数为p^n的域(§1.13)．斯坦尼茨(Steinitz)把这个结果推广到特征$p\neq0$的绝对代数域，就是下面习题所指出的．

6．**斯坦尼茨数**是所有素数 p_i 的形式积 $N=\Pi p_i^{k_i}$，其中 $k_i=0,1,2,\cdots$ 或 ∞．设 $M=\Pi p_i^{l_i}$ 是另一斯坦尼茨数，如果对一切i都有 $l_i\leqslant k_i$，则称M是N的因子($M|N$)．容易由此导出任何斯坦尼茨数的集族之最小公倍(L.C.M.)的定义．设Φ是特征为p的绝对代数域，定义 $\deg\Phi$ 为：Φ的元在素域($\cong I_p$)上的各最小多项式的次数的斯坦尼茨数的L.C.M.(注意，如果Φ是有限的，则 $|\Phi|=p^{\deg\Phi}$)．证明，对任意给定的素数p和斯坦尼茨数N，存在一个绝对代数域 $\Phi_{p,N}$ 其特征为p而

$$\deg\Phi_{p,N}=N$$

(提示：令r_n是N和$n!$的最高公因子，于是 $r_n|r_{n+1}$，$n=1,2,\cdots$．令 Φ_n 是基数为 p^{r_n} 的域．假设 $\Phi_n\subseteq\Phi_{n+1}\subseteq\cdots$，则 $\Phi_{p,N}=\cup\Phi_n$．)证明，任意两个有相同素特征和斯坦尼茨次数的绝对代数域同构．并证明，$\Phi_{p,M}$ 同构于 $\Phi_{p,N}$ 的一个子域当且仅当 $M|N$．

2．无限伽罗瓦理论　这一节中，我们把伽罗瓦理论的基本定理推广到某些无限维代数扩张域 P/Φ 上．我们假设P是Φ上可分多项式集Ω的一个分裂域．首先证明下述的

引理 1. P的任何有限子集含于有限维伽罗瓦子域 E/Φ 中.

证 设 f 是集 Ω 中有限个多项式乘积所成的多项式. 显然 P 包含 f 的分裂域 P_f/Φ. 我们知道, P_f 是 Φ 上有限维伽罗瓦域(定理 1.10). 显然,如果 f 和 g 都是 Ω 的多项式的乘积, 则 P_{fg} 是由 P_f 和 P_g 生成的 P的子域.于是,所有这些子域的并 $\cup P_f$ 是 Φ 上 P 的子域. 因为 $\cup P_i$ 包含每一 $g\in\Omega$ 的分裂域,显然 $\cup P_f = P$. 这就推出任何 $\rho_i\in P$ 必属于子域 P_{f_i}, 于是任何有限子集 $\{\rho_1, \rho_2, \cdots, \rho_m\}$ 包含在 Φ 上的有限维伽罗瓦子域 $P\Pi_{f_i}$ 中.

令 G 是 P/Φ 的伽罗瓦群. 下述定理实质上给出了伽罗瓦对应的前一半结果.

引理 2. $\Phi = I(G)$. 即 P 的 G 不变元只能是 Φ 的元.

证 我们只要证明: 若 $\rho\in P$, $\notin\Phi$, 则存在 Φ 上 P 的自同构 s 使 $\rho^s\neq\rho$. 由引理 1, ρ 含于 Φ 上有限伽罗瓦子域 E/Φ 中. 因为 $\rho\notin\Phi$, 所以存在 E/Φ 的伽罗瓦群的元 $\bar{s}$ 使 $\rho^{\bar{s}}\neq\rho$. 另一方面, P 是多项式集 Ω 在 E 上的分裂域, 于是由定理 2, E 的自同构 $\bar{s}$ 能延拓为 P/Φ 的自同构 s, 显然 $s\in G$, $\rho^s=\rho^{\bar{s}}\neq\rho$.

全部中间子域-子群间的对应关系在有限维情形下是成立的, 但在无限维情形下不成立. 作为例子, 我们考虑含 p 个元的域 $\Phi = I_p$ 的代数闭包 P, 因为 Φ 是完全的, $\Phi[x]$ 的所有多项式是可分的, 因此 P 是 $\Phi[x]$ 中可分多项式集 Ω 在 Φ 上的分裂域. 令 G 是 P/Φ 的伽罗瓦群, H 是由自同构 $\pi:\rho\to\rho^p$ (显然这是自同构)生成的子群. 因为满足 $\rho^p=\rho$ 的元 ρ 只能是 Φ 的 p 个元,所以 H 不变的子域 $I(H)$ 是 Φ. 下面证明 H 是 G 的真子群, 这样一来, G 有两个子群 G 和 H, 它们有相同的不变元子域. 为证这一点,设 p^e 是 p 的任意幂 ($e\geqslant 1$), 则 P 含有一个 p^e 阶子域 Φ_e. 我们还知道 $\Phi_e\subseteq\Phi_f$ 当且仅当 $e\mid f$ (§ 1.13). 设 l 是素数, Φ_{l^∞} 表示序列 $\Phi_l\subset\Phi_{l^2}\subset\Phi_{l^3}\subset\cdots$ 中的域的并,即知 Φ_{l^∞} 是 P 的一个真子域. P 是集 Ω 在 Φ_{l^∞} 上的分裂域,因此由引理 2 得知,存在 Φ_{l^∞} 上 P的自同构 s 满足 $s\neq 1$. 此处 s 不是自同构 π 的方幂, 否则若 $s=\pi^k$, 则 s 不变元的子域是满足 $\rho^{p^k}=\rho$ 的元的有限集, 这个集必

须包含 Φ_{l^∞}. 这是不可能的，因为 Φ_{l^∞} 是 P 的无限子域.

无限伽罗瓦理论这一类型的困难首先由戴得金在有理代数数域中觉察到，解脱这种困难的方法则为克鲁尔 (Krull) 所发现，他认为有必要把伽罗瓦对应限制在伽罗瓦群对某个拓扑的闭子群集，现在我们来定义它.

所需要的拓扑与卷 2 (中译本 p.223) 中关于向量空间到另一个向量空间的线性变换集的有限拓扑基本一致. 考虑域 P 到自身内的(单值)映射集 P^P. 如果 $(\xi_1, \xi_2, \cdots, \xi_m)$ 和 $(\eta_1, \eta_2, \cdots, \eta_m)$ 是 P 的元的有限序列，那末令 $O(\xi_i, \eta_i)$ 是 P^P 中满足 $\xi_i^s=\eta_i$ $(i=1, 2, \cdots, m)$ 的元 s 所成的子集. 各集 $O(\xi_i, \eta_i)$ 可以作为使 P^P 成为拓扑空间的开集的集的基(参看卷 2 的中译本 p. 223)，P^P 的拓扑叫作**有限拓扑**.

若 G 是 P^P 的任何子集，即 P 到自身内的映射的任一集，将 G 拓扑化，作为 P^P 的子空间. 我们特别要对 P/Φ 的伽罗瓦群 G 这样作. 现证以下事实：若 P 是 Φ 的代数扩张域，则 G 是 P^P 的闭子集. 设 $\bar{s}$ 属于 G 的闭包，且 $\xi, \eta \in P$, $\alpha \in \Phi$. 则存在 $s \in G$ 使 $\alpha^s=\alpha^{\bar{s}}$, $\xi^s=\xi^{\bar{s}}$, $\eta^s=\eta^{\bar{s}}$, $(\xi+\eta)^s=(\xi+\eta)^{\bar{s}}$, $(\xi\eta)^s=(\xi\eta)^{\bar{s}}$. 因为 $\alpha^s=\alpha$, $(\xi+\eta)^s=\xi^s+\eta^s$, $(\xi\eta)^s=\xi^s\eta^s$，而且 $\bar{s}$ 也有相同的关系，这就表明 $\bar{s}$ 是 P/Φ 到自身内的同构. 为了证明 $\bar{s}$ 是满射，我们令 ξ 是 P 的任意元，E 是 P/Φ 的子域，它由 ξ 在 Φ 上的最小多项式 $f(x)$ 在 P 内的所有根 ξ' 生成，显然 $[E:\Phi]<\infty$. 因为 $\bar{s}$ 是 P/Φ 到自身内的同构，所以 $E^{\bar{s}}\subseteq E$. 因此 $\bar{s}$ 的限制是 E/Φ 到自身的线性同构，所以这个映射是满射. 于是存在 $\eta\in E$ 使 $\eta^{\bar{s}}=\xi$. 所以 $\bar{s}$ 是 P/Φ 的自同构，于是 $\bar{s}\in G$，即 G 是闭的.

我们能够证明下述无限伽罗瓦理论的基本定理.

定理 4. 设 P/Φ 是系数在 Φ 中的可分多项式集 Ω 的分裂域，G 是 P/Φ 的伽罗瓦群. 和 G 的每一闭子群 H 相对应的 H 不变子域为 $E=I(H)$，和 Φ 上 P 的每一子域 E 相对应的 P 在 E 上的伽罗瓦群为 $A(E)$，则这两个对应是互逆的. 此外，闭子群 H 是 G 的不变子群当且仅当相应的 $E=I(H)$ 是 Φ 上的伽罗瓦域，此时

E/Φ 的伽罗瓦群同构于 G/H.

证　如果E是P/Φ的子域,则P是Ω在E上的分裂域. 因此若 $H=A(E)$ 是 P/E 的伽罗瓦群,则H是闭的,由引理2,

$$I(A(E))=E,$$

以下令H是G的闭子群, 且令 $E=I(H)$. 我们必须证明: 若s是 P/E 的自同构,则 $s\in H$. 因为H是闭的, 故只须证明s在H的闭包内, 即如果 $\rho_1,\rho_2,\cdots,\rho_n\in\mathrm{P}$, 则存在 $t\in H$使 $\rho_i^t=\rho_i^s$, $1\leqslant i\leqslant n$. 令 Λ/E 是 P/E 的有限维伽罗瓦子域,且包含 $\{\rho_i\}$ (引理1),则s和$t\in H$都把Λ映到自身内. 所以它们的限制是Λ/E 的伽罗瓦群的元,如果s与$t\in H$在Λ上的限制s'与t'都不重合, 则$t\in H$ 的限制所成群H'是Λ 在E上的伽罗瓦群的真子群. 于是存在元 $\xi\in\Lambda$, $\notin E$, 使 $\xi^t=\xi$ 对每一$t\in H$均成立. 这和 $E=I(H)$ 矛盾. 于是证明了第一个命题. 如果H是闭子群, $s\in G$, 则 $s^{-1}Hs$是闭的;如果$E=I(H)$, 则$E^s=I(s^{-1}Hs)$. 于是H是G的不变子群当且仅当 $E^s=E$ 对每一$s\in G$都成立. 若这一条件成立,则$s\in G$在E上的限制的集是E的自同构群$\bar{G}$, 其不变集是Φ. 因此E是Φ上的伽罗瓦扩张. 反之, 假设E是Φ上的伽罗瓦扩张,且$\bar{G}$是 E/Φ 的伽罗瓦群. 如果 $\varepsilon\in E$, $\bar{s}\in\bar{G}$, 则ε和$\varepsilon^{\bar{s}}$在Φ上有相同的最小多项式. 因此ε只有有限个共轭$\varepsilon^{\bar{s}}$, $\bar{s}\in\bar{G}$. 设这些共轭元为 $\varepsilon_1=\varepsilon,\varepsilon_2,\cdots,\varepsilon_r$, 则多项式

$$f(x)=\Pi(x-\varepsilon_i)$$

的系数在Φ中,且ε是 $f(x)=0$ 的根. 若 $s\in G$, 则 ε^s 也是

$$f(x)=0$$

的一个根,所以 $\varepsilon^s=\varepsilon_i\in E$. 因为$\varepsilon$是任意的,这就证明了$E^s\subseteq E$对一切$s\in G$成立. 因此$H$是$G$的不变子群. 因为$\mathrm{P}$是 $\Phi[x]$ 的多项式集在Φ上的分裂域, E/Φ 的任何自同构能够延拓为 P/Φ 的自同构. 由此易见,若E是Φ上的伽罗瓦扩张, 则映射 $s\to\bar{s}$(s在E上的限制) 是G到$\bar{G}$ 上的同态, 核是 $H=A(E)$, 故 $\bar{G}\cong G/H$.

习　题　27

1．证明定理4的假设可以改为：P/Φ 是可分的正规代数扩张．此处正规性由以下条件定义：如果 $f(x)$ 是 $\Phi[x]$ 中不可约多项式，且在P中有根，则 $f(x)$ 是 $P[x]$ 的一次因式之积(参考§1.18)．

2．拓扑空间称为**离散的**，假若每个子集都是开集．令P是Φ上可分多项式集的分裂域，G是P在Φ上的伽罗瓦群．证明G是离散的当且仅当 $[P:\Phi]<\infty$．

3．P，Φ和G如题2．利用每一 $\rho\in P$ 仅有有限个共轭这一事实及铁柯诺夫(Tychonoff)定理证明G是一个紧致群．

4．设P是域 $\Phi=I_p$ 的代数闭包，G是P在Φ上的伽罗瓦群，证明G是交换群．令 Φ_{l^∞} 是P的子域(l是素数，定义如正文)，π是限制在 Φ_{l^∞} 上的自同构 $\rho\to\rho^p$．证明 $\pi^{l^k}\to 1$，也就是说，若S是 Φ_{l^∞} 的任意有限子集，则存在正整数N使 $\xi^{\pi^{l^k}}=\xi$ 对一切 $\xi\in S$ 和 $k\geqslant N$ 成立．令 $m_1, m_2, \cdots$ 是整数序列，且对任何正整数k，存在N使 $r, s\geqslant N$ 时有 $m_r\equiv m_s \pmod{l^k}$．证明自同构序列 $\pi^{m_1}, \pi^{m_2}, \cdots$ 收敛于Φ上 Φ_{l^∞} 的自同构 σ，即 $\pi^{m_k}\sigma^{-1}\to 1$．

5．设G是域P中的自同构群，$\Phi=I(G)$，G是 P^P 的紧致子集．证明对每一 $\xi\in P$，集 $\{\xi^s|s\in G\}$ 是有限的．从而证明P是Φ上可分多项式集的分裂域，而且G是 P/Φ 的伽罗瓦群．

6．设G是 P/Φ 的伽罗瓦群，P是Φ上的代数扩张域，$\{G_\alpha\}$ 是在G中具有有限指数的不变子群的集族，证明 $\bigcap G_\alpha=1$．

7．设Φ是有限域，A是它的代数闭包．G是 A/Φ 的伽罗瓦群，证明G除1外，没有有限阶元．

8．设A_p 是含p个元的域 I_p 的代数闭包，G_p 是 A_p/I_p 的伽罗瓦群．证明，对任意素数p和q均有 $G_p\cong G_q$．

9．设 $P=\Phi(\xi_1, \xi_2, \cdots)$ 是无限个未定元的有理式所成的域，证明 P/Φ 的伽罗瓦群在有限拓扑中不是闭的．

3. 超越基　在卷1中曾经定义了Φ上域P的有限子集 $\{\xi_1, \xi_2, \cdots, \xi_n\}$ 在Φ上的代数无关性，这个定义在导言(p.4)中已重复过．现在把这个概念推广到任意子集：如果S的每一有限子集是代数无关的，则称集S是代数无关的．不是代数无关的集称为代数相关的；因此一个集是代数相关的当且仅当它含有一个非空的代数相关的有限子集．现将引入另一概念．在定理1中会看到，它和刚才所说的概念有密切的联系．

定义 1．　令S是Φ上P的子集，ρ是P的元；如果ρ在 $\Phi(S)$ 上是代数元，则称ρ**在Φ上和S代数相关**．

首先注意，如果ρ在Φ上和S代数相关而且$f(x)\in\Phi(S)[x]$是ρ在$\Phi(S)$上的最小多项式，则$f(x)$的系数含于子域$\Phi(F)$中，此处F是S的有限子集．因此，ρ在Φ上和S代数相关当且仅当对S的某一有限子集F有这个性质．

定理5. 域P/Φ的一个非零子集S在Φ上代数相关当且仅当存在元$\xi\in S$，它在Φ上和余集$S-\{\xi\}$代数相关．

证 我们所作的注释表明只要对S是有限集的情形加以证明就行了．设$S=\{\xi_1,\xi_2,\cdots,\xi_n\}$．假定所说条件成立，则可设$\xi_n$是$\Phi(\xi_1,\xi_2,\cdots,\xi_{n-1})$上的代数元．令

$$f(x)\in\Phi(\xi_1,\cdots,\xi_{n-1})[x]$$

是ξ_n在$\Phi(\xi_1,\cdots,\xi_{n-1})$上的最小多项式，$\beta_1,\beta_2,\cdots,\beta_m$是它的系数，而$\Phi(\xi_1,\cdots,\xi_{n-1})$的每一元有$g(\xi_1,\cdots,\xi_{n-1})h(\xi_1,\cdots,\xi_{n-1})^{-1}$形式，其中$g,h\in\Phi[x_1,\cdots,x_{n-1}]$，$x_i$是未定元，$h(\xi_1,\cdots,\xi_{n-1})\neq 0$．特别是$\beta_i=g_i(\xi_1,\cdots,\xi_{n-1})h_i(\xi_1,\cdots,\xi_{n-1})^{-1}$，$h_i(\xi_1,\cdots,\xi_{n-1})\neq 0$．设$h(x_1,\cdots,x_{n-1})=\Pi h_i(x_1,\cdots,x_{n-1})$以及

$$\begin{aligned}F(x_1,\cdots,x_n)=h(x_1,\cdots,x_{n-1})\{x_n^m\\+g_1(x_1,\cdots,x_{n-1})h_1(x_1,\cdots,x_{n-1})^{-1}x_n^{m-1}+\cdots\\+g_m(x_1,\cdots,x_{n-1})h_m(x_1,\cdots,x_{n-1})^{-1}\},\end{aligned}$$

则F是$\Phi[x_1,\cdots,x_n]$中的非零元，其中x_i是未定元，且有$F(\xi_1,\cdots,\xi_n)=0$．这就表示ξ_i是代数相关的．相反地，假设存在一非零多项式$F(x_1,\cdots,x_n)\in\Phi[x_1,\cdots,x_n]$使$F(\xi_1,\cdots,\xi_n)=0$，总的来说这些$\xi_i$在$\Phi$上代数相关，不妨设$n$是满足上述假设的最小数，则可写成

$$\begin{aligned}F(x_1,\cdots,x_n)=f_0(x_1,\cdots,x_{n-1})x_n^m\\+f_1(x_1,\cdots,x_{n-1})x_n^{m-1}+\cdots\\+f_m(x_1,\cdots,x_{n-1}),\end{aligned}$$

此处$f_0\neq 0$，$m\geqslant 1$．因为n是最小的，$f_0(\xi_1,\cdots,\xi_{n-1})\neq 0$，则

$$f(x)=x^m+\sum_1^m f_i(\xi_1,\cdots,\xi_{n-1})f_0(\xi_1,\cdots,\xi_{n-1})^{-1}x^{m-i}$$

是 $\Phi(\xi_1,\cdots,\xi_{n-1})[x]$ 的一个非零元，它使 $f(\xi_n)=0$ 成立，因此 ξ_n 和 $\xi_1,\cdots,\xi_{n-1}$ 是代数相关的.

域 P/Φ 中代数相关性是 P 的元与 P 的子集之间的关系的一种特殊类型. 与此类似的另一种关系是向量空间中的向量与子集的线性相关性，我们还会遇到其它情形. 因此有必要对这些关系作公理化的处理. 为此可考虑一任意集 P. P 的元与 P 的子集 S 之间的关系 $<(\xi<S)$ 叫作**相关关系**,如果以下条件成立:

I. 若 $\xi\in S$, 则 $\xi<S$.

II. 若 $\xi<S$, 则 $\xi<F$ 对 S 的某个有限子集 F 成立.

III. 若 $\xi<S$, 且 S 中每一元 η 满足 $\eta<T$, 则 $\xi<T$.

IV. 若 $\xi<S$ 且 $\xi\nless S-\{\eta\}$, 此处 $\eta\in S$, 则

$$\eta<(S-\{\eta\})\cup\{\xi\}\ (\text{替换公理}).$$

今设 P 是 Φ 上的域,对于 P 中元 ξ 和 P 的子集 S, $\xi<S$ 意味着 ξ 在 Φ 上和 S 代数相关,则有

定理 6. P/Φ 的代数相关性是 I—IV 意义下的相关关系.

证 I. 这是显然的. II. 在前面已经证明. III. 令 ξ 是 $\Phi(S)$ 上的代数元,设每一 $\eta\in S$ 是 $\Phi(T)$ 上的代数元. 考虑 P 中 $\Phi(T)$ 上的代数元所成的子集 A. 我们知道 A 是 $P/\Phi(T)$ 的子域，而且在 P 中是代数封闭的. 令 $S\subseteq A$, ξ 是 $\Phi(S)$ 上的代数元,所以 ξ 也是 A 上的代数元. 因此 $\xi\in A$, $\xi<T$. IV. 设 $\xi<S$, 而 $\xi\nless T=S-\{\eta\}$, $\eta\in S$. 令 $E=\Phi(T)$, 则 ξ 是 E 上的超越元又是 $E(\eta)$ 上的代数元. 因此存在多项式 $f(x,y)\in E[x,y]$ 使 $f(x,y)\neq 0$, 而 $f(\xi,\eta)=0$, 这里 x, y 是 E 上的未定元. 将 $f(x,y)$ 写成 $f(x,y)=a_0(x)y^m+a_1(x)y^{m-1}+\cdots+a_m(x)$,这里 $a_i(x)\in E[x]$, 且 $a_0(x)\neq 0$.因为 ξ 是 E 上的超越元,所以 $a_0(\xi)\neq 0$ 且 $m>0$. 多项式 $f(\xi,y)$ 是属于 $E(\xi)[y]$ 的非零多项式, η 是 $f(\xi,y)=0$ 的根. 因此 η 是 $E(\xi)$ 上的代数元，从而得到 η 是 $\Phi(T\cup\{\xi\})$ 上的代数元,所以 $\eta<T\cup\{\xi\}$.

现在回到相关关系的一般理论上来. 和前面一样，设 P 是任意集,我们定义 P 的子集 S (关于$<$)是**无关的**,如果不存在 $\xi\in S$

和 $S-\{\xi\}$ 相关。于是我们就有以下的结论

引理. 设 B 是无关的,而 ξ 和 B 不是相关的,则 $B\cup\{\xi\}$ 是无关的。

证 否则,有 $\eta\in B$ 使 $\eta<(B\cup\{\xi\})-\{\eta\}$因为 $\eta\not<B-\{\eta\}$. 由替换公理得到 $\xi<B=(B-\{\eta\})\cup\{\eta\}$, 这与假设矛盾.

P的一个子集 B 称为 P (关于<)的一个基,如果: (1) B 是无关的, (2) P的每一元 ξ 和 B[1] 相关. 相关关系的主要结果如下:

基定理. 集P有一个基,P的任何两个基有相同的基数.

证 为了证明基的存在性,我们考虑P的那些无关子集所成的集族 I (I 可能只含空集)利用包含关系序化 I. 如果 $\{S\}$ 是 I 的线性有序子集,则 $\cup S$ 属于 I. 否则,有 $\xi\in\cup S$ 和 $\cup S-\{\xi\}$ 相关,则 $\xi<F$, 这里 F 是$\cup S-\{\xi\}$ 的有限子集,而且 $F\cup\{\xi\}$ 也是有限子集但不是无关的. 因为 $\{S\}$ 是线性有序的, 则对某个 $T\in\{S\}$ 有 $F\cup\{\xi\}\subseteq T$. 这与 T 是无关集的假设矛盾. 可见 I 是可归纳的, 于是由卓伦引理, I 中有极大元 B. 设 ξ 是 P的任意元,则 ξ 和 B 相关. 否则,由引理得 $B\cup\{\xi\}$ 是无关的, 与 B 的极大性矛盾. 所以P中每个元 ξ 和 B 相关. 故 B 是一个基.

设 B 和 C 是P的两个基. 我们要证明基数 $|B|=|C|$. 首先假设 B 是有限的,即 $B=\{\beta_1,\beta_2,\cdots,\beta_n\}$. 可以断言,在 $\gamma=\gamma_1\in C$ 使 γ 和 $\{\beta_2,\cdots,\beta_n\}$ 不相关. 否则由 III, P 的每一元素和 $\{\beta_2,\cdots,\beta_n\}$ 相关,特别是 β_1 也有这个性质,则与 B 的无关性矛盾. 今设 γ_1 和 $\{\beta_2,\cdots,\beta_n\}$ 不相关, 则 $\{\gamma_1,\beta_2,\cdots,\beta_n\}$ 是无关的. 由替换公理得到 $\beta_1<\{\gamma_1,\beta_2,\cdots,\beta_n\}$, 因此每一

$$\beta_i<\{\gamma_1,\beta_2,\cdots,\beta_n\}.$$

于是 $\{\gamma_1,\beta_2,\cdots,\beta_n\}$ 是一个基. 重复这个步骤得到 $\gamma_2\in C$ 使 $\{\gamma_1,\gamma_2,\beta_3,\cdots,\beta_n\}$ 是一个基. 连续使用这一方法得到一个基 $\{\gamma_1,\cdots,\gamma_n\}$, 这是 C 的一个子集且与 B 有相同的基数. 因为 C

---

1) 此 B 原文误为 S. ——译者注.

是无关的，所以这些γ是C的所有元，故 $|C| = |B|$. 以下假设 $|C|$ 和 $|B|$ 是无限的，可以采用洛尉 (Lôwig) 的计数论证(参看卷 2，中译本 p. 216). 设 $\gamma \in C$，则γ和B的有限子集B_γ相关. 于是 $|\{B_\gamma\}| \leqslant |C|$，而且

$$\left|\bigcup_{\gamma \in C} B_\gamma\right| \leqslant \aleph_0 |C| = |C|.$$

其次我们还有 $\cup B_\gamma = B$. 否则，有$\beta \in B$，$\notin \cup B_\gamma$. 因为$\beta < C$而且每一$\gamma \in C$满足 $\gamma < \cup B_\gamma$，我们有 $\beta < \cup \beta_\gamma$，但 $\cup \beta_\gamma$ 不包含β，这与B的无关性矛盾. 所以 $\cup B_\gamma = B$，由上面基数的关系式给出 $|B| \leqslant |C|$，再由对称性 $|C| \leqslant |B|$. 所以 $|B| = |C|$.

这个结果特别可用到P/Φ的代数相关性去，此时基B是 P/Φ 的代数无关元的集，且使P的每一元ξ和B是代数相关的. 这样的集B 叫作 P/Φ 的一个超越基，它的基数(所有基的基数相同)叫作 P/Φ 的超越次数 (tr. d.)，所以扩张 P/Φ 是代数的当且仅当P在Φ上的超越基是空集，即当且仅当超越次数为 0. 如果P在Φ上有超越基B使 $P = \Phi(B)$，则称P是Φ的纯超越扩张. 超越基的存在性定理可解释如下：每一个域都能作为基域Φ的纯超越扩张 $\Phi(B)$ 的代数扩张得来. 设 $x_1, x_2, \cdots, x_r$ 是未定元，则代数 $\Phi[x_1, \cdots, x_r]$ 的分式域是Φ的有超越基 $\{x_i\}$ 的纯超越扩张 $\Phi(x_1, \cdots, x_r)$. 显然，次数 $r < \infty$的纯超越扩张和 $\Phi(x_1, \cdots, x_r)$ 实际上是相同的.

在代数几何中特别令人感兴趣的是域 $P = \Phi(\xi_1, \xi_2, \cdots, \xi_n)$，它是由元$\xi_i$的有限集在基域$\Phi$上生成的. 如果$B$是集 $\{\xi_1, \xi_2, \cdots, \xi_n\}$ 的极大代数无关子集，则B是超越基. 可以假设 $B = \{\xi_1, \xi_2, \cdots, \xi_r\}$，形为 $P = \Phi(\xi_1, \xi_2, \cdots, \xi_n)$ 的域叫作Φ上的代数函数域，超越次数 $r (\leqslant n)$ 叫作P的变元个数. 若 $\{\xi_1, \cdots, \xi_r\}$ 是超越基，则P是 $\Phi(\xi_1, \xi_2, \cdots, \xi_r)$ 的有限维扩张. 如果这是 $\Phi(\xi_1, \xi_2, \cdots, \xi_r)$ 的有限维扩张，则关于本原元的一个定理表明，对适当的 $\eta \in P$，有 $P = \Phi(\xi_1, \cdots, \xi_r, \eta)$. 这在特征为 0 的情形总

是如此，我们在§5将看到在简单的条件下代数函数域有基 $\{\xi_i\}$ 存在，使P是 $\Phi(\xi_1, \xi_2, \cdots, \xi_r)$ 上的可分代数扩张。

习　题　2B

1. 证明：如果C是 P/Φ 的子集，使得P的每一元和C是代数相关的，则C包含一个超越基。并证明，如果D是 P/Φ 的一个代数无关子集，则D能被嵌入一个超越基中。

2. 设 E/Φ 是 P/Φ 的子域。证明超越次数 $\text{tr.d.}P/E \leqslant \text{tr.d.}P/\Phi$，而且

$$\text{tr.d.}E/\Phi \leqslant \text{tr.d.}P/\Phi.$$

3. 设 E/Φ 是 P/Φ 的子域，B和C分别是 E/Φ 和 P/E 的超越基。证明$B\cup C$是 P/Φ 的一个超越基。从而证明公式

$$\text{tr.d.}P/\Phi = \text{tr.d.}P/E + \text{tr.d.}E/\Phi. \tag{1}$$

注意第2题是此式的一个推论。（提示：因为E在 $\Phi(B)$ 上是代数的，E/Φ 和 $\Phi(C)$ 生成的子代数是一个域，它在 $\Phi(B, C)$ 上是代数的（见第一章第九节的第二段）。因此 $E(C)$ 在 $\Phi(B, C)$ 上是代数的。

4. 证明：若Φ是特征$\neq 3$的域且 $P = \Phi(\xi, \eta)$，这里ξ是超越的而且 $\eta^3 + \xi^3 = 1$，则P在Φ上不是纯超越的。

5. 设P是复数域，Φ是有理数子域。证明：$\text{tr.d.}P/\Phi = C = |P|$。并证明：若$B$是 P/Φ 的超越基，则B的任意1—1满射可以延拓为 P/Φ 的一个自同构。从而证明P的自同构与1—1满射的个数相同。

6. 证明：如果P在Φ上是有限生成的，则 E/Φ 的任何子域也如此。

4. 吕洛斯（Lüroth）定理　纯超越扩张 $P = \Phi(\xi_1, \xi_2, \cdots, \xi_r)$ 看起来好象是最简单的一类扩张域，然而关于这种扩张却容易提出一些难于回答的问题。特别是 $r > 1$ 时关于 P/Φ 的子域问题。在 $r = 1$ 时，这种情形比较简单，本节就来讨论这个问题。

设 $P = \Phi(\xi)$，ξ是超越元，η是P的元但不含于Φ中。令 $\eta = f(\xi)g(\xi)^{-1}$，这里 $f(\xi)$ 和 $g(\xi)$ 是ξ的正次数而无公因子的多项式。不妨设 $f(\xi) = \alpha_0 + \alpha_1\xi + \cdots + \alpha_n\xi^n$，$g(\xi) = \beta_0 + \beta_1\xi + \cdots + \beta_n\xi^n$。这里或是 $\alpha_n \neq 0$ 或是 $\beta_n \neq 0$，所以n是f和g的较大次数。关系 $\eta = f(\xi)g(\xi)^{-1}$ 给出 $f(\xi) - \eta g(\xi) = 0$，且

$$0 = (\alpha_n - \eta\beta_n)\xi^n + (\alpha_{n-1} - \eta\beta_{n-1})\xi^{n-1} + \cdots + (\alpha_0 - \eta\beta_0).$$

因为 α_n 或 $\beta_n \neq 0$，$\eta \notin \Phi$，故 $\alpha_n - \eta\beta_n \neq 0$，由此可见 ξ 是 n 次方程 $\sum_0^n (\alpha_i - \eta\beta_i)x^i = 0$ 的一个根，其系数在 $\Phi(\eta)$ 中．我们再证 $\sum_0^n (\alpha_i - \eta\beta_i)x^i$ 在 $\Phi(\eta)[x]$ 中是不可约的：首先，η 显然是 Φ 上的超越元．这是因为 ξ 是 $\Phi(\eta)$ 上的代数元．如果 η 是 Φ 上的代数元，则推得 ξ 也是 Φ 上的代数元，这与假设矛盾．环

$$\Phi[\eta, x] = \Phi[\eta][x]$$

是两个未定元素 η，x 的多项式环，我们知道这是高斯环，即在 $\Phi[\eta, x]$ 中唯一分解为不可约元的定理成立(卷 I，中译本 p.117)．还知道如果 $\Phi[\eta, x]$ 中含 x 的正次数多项式在 $\Phi[\eta, x]$ 中是不可约的，那么它在 $\Phi(\eta)[x]$ 也是不可约的．今

$$f(\eta, x) = \Sigma(\alpha_i - \eta\beta_i)x^i = f(x) - \eta g(x)$$

是 η 的一次多项式．因此若 $f(\eta, x)$ 在 $\Phi(\eta)[x]$ 中是可约的，则它有含 x 的正次数因子 $h(x)$，这就推得 $f(x)$ 和 $g(x)$ 都能被 $h(x)$ 除尽，与假设矛盾．因此证明了 $f(\eta, x)$ 在 $\Phi(\eta)[x]$ 中不可约．于是 ξ 是 $\Phi(\eta)$ 上的 n 次代数元．这就证明了

定理 7. 设 $P = \Phi(\xi)$，ξ 是 Φ 上的超越元，η 是 P 的元但不在 Φ 中．记 $\eta = f(\xi)g(\xi)^{-1}$，这里 $f(\xi)$ 和 $g(\xi)$ 是 ξ 的无正次数公因式的多项式．设 $n = \max(\deg f, \deg g)$，则 ξ 是 $\Phi(\eta)$ 上的代数元，$[\Phi(\xi):\Phi(\eta)] = n$．而且 $f(x, \eta) = f(x) - \eta g(x)$ 在 $\Phi(\eta)[x]$ 中不可约．

这个结果能使我们决定 $\Phi(\xi)$ 在 Φ 上的自同构．这个自同构完全由生成元 ξ 的象 η 所确定．若 $\xi \to \eta$，则

$$u(\xi)v(\xi)^{-1} \to u(\eta)v(\eta)^{-1},$$

u，v 是 ξ 的多项式．显然，若 η 是 ξ 在自同构下的象，则 $\Phi(\eta) = \Phi(\xi)$．若 $\eta = f(\xi)g(\xi)^{-1}$，则 $[\Phi(\xi): \eta(\xi)] = n = \max(\deg f, \deg g)$．这就证明了 $\Phi(\eta) = \Phi(\xi)$ 当且仅当 $\max(\deg f, \deg g) = 1$．于是有

$$\eta = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}, \tag{2}$$

这里 $\alpha \neq 0$ 或 $\gamma \neq 0$，$\alpha\xi + \beta$ 与 $\gamma\xi + \delta$ 没有正次数的公因式。容易看出这些条件等价于一个条件：

(3) $$\alpha\delta - \beta\gamma \neq 0.$$

如果这个条件成立，则 $\Phi(\eta) = \Phi(\xi)$，且映射

$$u(\xi)v(\xi)^{-1} \to u(\eta)v(\eta)^{-1}$$

是 P/Φ 的自同构。

条件 (3) 等价于说矩阵

(4) $$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

是非奇异的。和每个这样的矩阵相联系的 Φ 上 $\Phi(\xi)$ 的自同构使 $\xi \to \eta$，η 由 (2) 给出。直接验证非奇异矩阵到相应的自同构内的映射是群同态，其核是满足 $(\alpha\xi + \beta)(\gamma\xi + \delta)^{-1} = \xi$，或

$$\alpha\xi + \beta = \xi(\gamma\xi + \delta)$$

的矩阵 $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ 的集。这就推得 $\gamma = 0$，$\beta = 0$，$\alpha = \delta$。因此核是纯量矩阵 $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \neq 0$ 的集。至此显见，$\Phi(\xi)$ 的自同构群同构于 2×2 阶非奇异矩阵群 $L(\Phi, 2)$ 关于纯量矩阵子群的商群。这个商群称为**射影群** $PL(\Phi, 2)$。

现在考虑 $\Phi(\xi)/\Phi$ 的任意子域 E。不妨设 $E \neq \Phi$。E 含有不在 Φ 中的元 η，$P = \Phi(\xi)$ 在 $\Phi(\eta)$ 上是代数的，因此在 $E \supseteq \Phi(\eta)$ 上是代数的。设 ξ 在 E 上的最小多项式是

$$f(x) = x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n.$$

γ_i 形为 $\mu_i(\xi)\nu_i(\xi)^{-1}$，其中 μ_i，ν_i 是超越元 ξ 的多项式。用 ξ 的一个适当多项式乘 $f(x)$ 得到 $\Phi[\xi, x]$ 中的一个多项式

(5) $$f(\xi, x) = c_0(\xi)x^n + c_1(\xi)x^{n-1} + \cdots + c_n(\xi),$$

其中 ξ，x 是未定元。这是 x 的本原多项式，即 $c_i(\xi)$的最高公因式为 1。我们还有各 $\gamma_i = c_i(\xi)c_0(\xi)^{-1} \in E$，但因 ξ 在 Φ 上是超越的，所以这些元不全在 Φ 中。因此 γ 中有一元形为：$\gamma = g(\xi)h(\xi)^{-1}$，这里 $g(\xi)$，$h(\xi)$没有正次数公因子，$\max(\deg g, \deg h) = m > 0$。前面曾经看到 $g(x) - \gamma h(x)$ 在 $\Phi(\gamma)[x]$ 中是不可约的，

$$[\mathrm{P}:\Phi(\gamma)]=m.$$

因为 $E\supseteq\Phi(\gamma)$，$[\mathrm{P}:E]=n$，显然 $m\geqslant n$. 我们要证明 $m=n$，从而证明 $E=\Phi(\gamma)$.

因为 ξ 是 $g(x)-\gamma h(x)=0$ 的根，这个多项式的系数在 E 中，在 $E[x]$ 中有 $g(x)-\gamma h(x)=f(x)q(x)$. 已知

$$\gamma=g(\xi)h(\xi)^{-1}.$$

我们可以将 f 和 q 的系数用 ξ 的有理式表示，然后乘以适当的 ξ 多项式得到 $\Phi[\xi,x]$ 中的关系式

$$k(\xi)[g(x)h(\xi)-g(\xi)h(x)]=f(\xi,x)q(\xi,x), \tag{6}$$

这里 $f(\xi,x)$ 是由 (5) 给出的本原多项式，于是 $k(\xi)$ 是 $q(\xi,x)$ 的因子，消去以后，可以假设关系式为

$$g(x)h(\xi)-g(\xi)h(x)=f(\xi,x)q(\xi,x). \tag{7}$$

其左边 ξ 的次数至多为 m，根据对称性，左边关于 x 的次数也至多是 m. 另一方面 $f(\xi,x)$ 关于 x 的次数为 n. 于是 $m=n$，除非左边是零. 而这将推出 $h(\xi)=\alpha g(\xi)$，$\alpha\in\Phi$；与

$$g(\xi)h^{-1}(\xi)=\gamma\notin\Phi$$

矛盾. 这样我们必有 $m=n$，和 $E=\Phi(\gamma)$. 如前所知，$E\supset\Phi$ 意味着 γ 是超越元. 我们就证明了以下:

定理 8（吕洛斯）. 设 $\mathrm{P}=\Phi(\xi)$，ξ 是 Φ 上的超越元，则任何子域 $E\supset\Phi$ 也是单超越扩张：$E=\Phi(\gamma)$，γ 是超越元.

吕洛斯定理对于超越次数 $r>1$ 的纯超越扩张 P/Φ 是无效的. 这方面的最好结果是卡斯特罗努禾-沙利斯基 (Castelnuovo-Zariski) 定理：如果 Φ 是代数封闭的且 $r=2$，若 P/E 是可分的、且 E/Φ 的超越次数等于2，则 E/Φ 是纯超越扩张[1].

习　题　29

1. 证明：如果 $\mathrm{P}=\Phi(\xi,\eta)$，$\xi$ 是超越元而且 $\eta^2+\xi^2=1$，则 P 是纯超越扩张.
2. 设 Φ 是有限域，$|\Phi|=q=p^m$. 求 $\Phi(\xi)/\Phi$ 的伽罗瓦群的阶，其中 ξ 是超

1) 参看 O. 沙利斯基，有理性 $P_a=P_2=0$ 的 Castelnuovo 判别法，*Illinois Jour. of Math.*, Vol. 2(1958), pp. 303—315.——著者注.

越元.

3. 给出 $\Phi[\xi]$ 的没有单一生成元的子代数例子 (ξ 是超越元).

4. 设 $P=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$, ξ_i 是代数无关的; 设 Σ 是 P 的对称元所成的子域,即 Σ 是在所有自同构 $A(\sigma)$: $\xi_i^{A(\sigma)}=\xi_{i\sigma}$ 之下不变的元的全体,其中 σ 是 $1,2,\cdots,m$ 的置换. 证明, Σ 是超越次数为 m 的纯超越扩张. 对子域 $\Delta\supseteq\Sigma$ 证明同样的结论,Δ 是在所有自同构 $A(\sigma)$ 之下不变的元所成之子域,而其中 σ 是交错群的元素.

(还不知道这结论对 S_m 的任一子群 G 是否成立.)

5. 线性不相交性及可分超越基

设 Φ 的特征 $p\neq 0$, $P=\Phi(\xi,\eta)$, 这里 ξ 是超越元且 $\eta^p=\xi$, 则 $\{\xi\}$ 是 P/Φ 的超越基,而 P 在 $\Phi(\xi)$ 上是不可分的. 另一方面, $P=\Phi(\eta)$ 在 P 上可分. 这个简单例子表明扩张的某个超越基 B 可能优于其他的基, 它能使 $P/\Phi(B)$ 是可分代数扩张. 还要指出, 这样的基不一定都存在, 例如 P/Φ 是代数扩张但不一定是 Φ 上的可分扩张. P/Φ 的一个超越基 B 称为**可分超越基**,如果 P 是 $\Phi(B)$ 上的可分代数扩张. 如果 P/Φ 有这样的基,则称 P/Φ 是**可分生成的**. 本节将得到一个 P/Φ 是可分生成的判别法. 它以下面重要概念为基础.

定义 2 设 E_1 和 E_2 是任意域 P/Φ 的子代数. 称 E_1 和 E_2 在 Φ 上是**线性不相交的**, 假若由 E_1 和 E_2 生成的子代数 E_1E_2 是张量积 $E_1\otimes_\Phi E_2$. 更精确地说就是 $E_1\otimes_\Phi E_2$ 到 E_1E_2 内的典范同态 $\varepsilon_1\otimes\varepsilon_2\to\varepsilon_1\varepsilon_2$ 是一个同构(见导言 §.3).

回顾导言中得到的 $E_1E_2=E_1\otimes_\Phi E_2$ 的条件是有好处的, 首先我们知道, 它的一个充分条件是 E_1 和 E_2 分别存在在 Φ 上的基 (u_α), (v_β) 使 $(u_\alpha v_\beta)$ 是 E_1E_2 在 Φ 上的基. 因为子代数 E_1E_2 的每一元总是元 $u_\alpha v_\beta$ 的线性组合. 可见 $E_1E_2=E_1\otimes_\Phi E_2$ 的充分条件是存在 E_1/Φ 和 E_2/Φ 的基 (u_α), (v_β) 使 $\{u_\alpha v_\beta\}$ 是 Φ 无关的. 假如 E_1 是 P/Φ 的子域, 若 E_2 有在 Φ 上的基 (v_β), 使 (v_β) 是 E_1 无关的,则 $E_1E_2=E_1\otimes_\Phi E_2$.

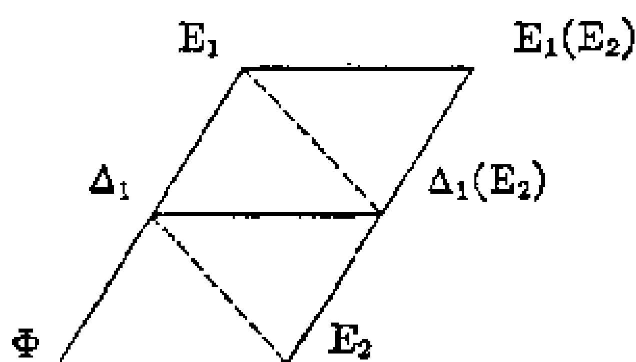
反之, 假若 E_1 和 E_2 是线性不相交的子代数. (u_α) 是 E_1/Φ 的任一个基 (v_β) 是 E_2/Φ 的任一个基, 则 $(u_\alpha v_\beta)$ 是 E_1E_2/Φ 的基. 类似的, 若 E_1 是子域, 则 (v_β) 是 E_1E_2/E_1 的基. 我们还注意到, 子代数 E_1 和 E_2 的线性不相交性意味着: 若 $\{u_\alpha\}$ 是 E_1/Φ

的线性无关子集，$\{v_\beta\}$ 是 E_2/Φ 的线性无关子集，则 $\{u_\alpha v_\beta\}$ 是 Φ 无关的.

其次注意到，E_1 和 E_2 是 Φ 上线性不相交子代数当且仅当分别由 E_1 和 E_2 生成的子域 Q_1 和 Q_2 在 Φ 上是线性不相交的. 因为若 Q_1 和 Q_2 有此性质，则 E_1 和 E_2 也有. 因为按我们的判别法，线性不相交代数的子代数也是线性不相交的. 反之，假如 E_1 和 E_2 是线性不相交的，令 $\xi_1, \xi_2, \cdots, \xi_m$ 是 Q_1 的 Φ 无关元，$\eta_1, \eta_2, \cdots, \eta_n$ 是 Q_2 的 Φ 无关元. 我们可以写成 $\xi_i = \xi_i'\xi^{-1}$，$\eta_j = \eta_j'\eta^{-1}$，这里 $\xi_i', \xi \in E_1$，$\eta_j', \eta \in E_2$. 则 $\{\xi_1', \xi_2', \cdots, \xi_m'\}$ 是 E_1 的 Φ 无关子集，$\{\eta_1, \eta_2, \cdots, \eta_n\}$ 是 E_2 的 Φ 无关子集. 所以 $\xi_i'\eta_j'$ 这 mn 个元是 Φ 无关的. 从而 $\xi_i\eta_j$ 也是 Φ 无关的. 这就得到 Q_1 和 Q_2 在 Φ 上是线性不相交的.

我们感兴趣的是 P 的子域. 为要逐步证明线性不相交性. 需要下面引理.

引理. 设 E_1 和 E_2 是 P/Φ 的子域，Δ_1 是 E_1/Φ 的子域，则 E_1 和 E_2 在 Φ 上线性不相交当且仅当以下两个条件成立：(1) Δ_1 和 E_2 在 Φ 上线性不相交及 (2) 域 $\Delta_1(E_2)$ 和 E_1 在 Δ_1 上线性不相交.



证　设 (1) 和 (2) 成立. 令 (u_α) 是 E_2/Φ 的基. 由 (1) 得 u_α 在 Δ_1 上线性无关. 而这些元含于 $\Delta_1(E_2)$ 中，由 (2) $\Delta_1(E_2)$ 与 E_1/Δ_1 在 Δ_1 上是线性不相交的，所以 u_α 在 E_1 上是线性无关的，故 E_1 和 E_2 在 Φ 上是线性不相交的. 反之，设 E_1 和 E_2 在 Φ 上线性不相交，显然 Δ_1 和 E_2 在 Φ 上线性不相交，即 (1) 成立. 由假设知道如果 (u_α) 是 E_1 在 Δ_1 上的基，(v_β) 是 Δ_1 在 Φ 上的基，

(w_γ) 是 E_2 在 Φ 上的基，则 $(u_\alpha v_\beta w_\gamma)$ 是 E_1E_3 在 Φ 上的基．因此，若有关系式 $\Sigma c_i u_{\alpha_i} = 0$，$c_i \in E_2\Delta_1$，则每一个 $c_i = 0$．今设 $\Sigma \delta_i u_{\alpha_i} = 0$，$\delta_i \in \Delta_1(E_2)$，$\delta_i$ 可写成 $\delta_i = c_i d^{-1}$，c_i，$d \in E_2\Delta_1$，则得到 $\Sigma c_i u_{\alpha_i} = 0$，$c_i = 0$ 及 δ_i[1] $= 0$．这就证明了 E_1/Δ_1 的基 (u_α) 是 $\Delta_1(E_2)$ 无关的．从而 E_1 与 $\Delta_1(E_2)$ 在 Δ_1 上是线性不相交的．

现在着手研究线性不相交性和可分性．设 P 是特征 $p \neq 0$ 的域 Φ 之扩张域．考察 P 的代数闭包 A（它包含 Φ 的一个代数闭包），A 中满足 $\gamma^p \in \Phi$ 的元 γ 所成的子集 $\Phi^{p^{-1}}$．这是 Φ 上的子域．我们对 P 和 $\Phi^{p^{-1}}$ 在 Φ 上的线性不相交性感兴趣．在研究这一问题时，注意到以下简单准则是有用的：集 $\{\rho_1, \rho_2, \cdots, \rho_n\}$ $(\rho_i \in \mathrm{P})$ 是 $\Phi^{p^{-1}}$ 无关的当且仅当 $\{\rho_1^p, \rho_2^p, \cdots, \rho_n^p\}$ 是 Φ 无关的；因为假设 $\Sigma \beta_i \rho_i = 0$，$\beta_i \in \Phi^{p^{-1}}$，则 $\Sigma \alpha_i \rho_i^p = 0$，$\alpha_i = \beta_i^p \in \Phi$．另一方面，如果 $\Sigma \alpha_i \rho_i^p = 0$，$\alpha_i \in \Phi$，则由于 A 包含 Φ 的一个代数闭包，$\alpha_i = \beta_i^p$，$\beta_i \in \Phi^{p^{-1}}$．故有 $\Sigma \beta_i^p \rho_i^p = 0$．因此 $(\Sigma \beta_i \rho_i)^p = 0$ 和 $\Sigma \beta_i \rho_i = 0$．显然在这两种情形中 $\alpha_i = 0$ 当且仅当 $\beta_i = 0$．现在建立以下准则

定理 9. 如果 P 是 Φ 的代数扩张(可能是无限维的)，则 P 在 Φ 上是可分的当且仅当 P 和 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交．

证　我们知道，P 在 Φ 上的代数元 ρ 是可分元当且仅当 $\rho \in \Phi(\rho^p)$（§1.9 的引理 2），先设 P 和 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交且 $\rho \in \mathrm{P}$，

$$[\Phi(\rho):\Phi] = n.$$

则 $(1, \rho, \rho^2, \cdots, \rho^{n-1})$ 是 $\Phi(\rho) = \Phi[\rho]$ 的基，因此这些元是 $\Phi^{p^{-1}}$ 无关的．而且 $1, \rho^p, \rho^{2p}, \cdots, \rho^{(n-1)p}$ 是 Φ 无关的．这些元共有 n 个且均含于 $\Phi(\rho)$ 中，故是 $\Phi(\rho)$ 的一个基．由此得到 $\rho \in \Phi(\rho^p)$，故 ρ 在 Φ 上是可分的．反之，假设 P 在 Φ 上是可分的，令 $\{\rho_1, \cdots, \rho_n\}$ 是 P 的 Φ 无关的有限子集．我们可以将这个子集嵌入有限维子域 E/Φ 中，且可替 E/Φ 选择一个基 $(\rho_1, \cdots, \rho_n,$

---

1) 原文误为 $d_i = 0$，特更正．——译者注．

$\rho_{n+1}, \cdots, \rho_q$). E 的任何元 ε 都是 $\rho_j(1 \leqslant j \leqslant q)$ 的一个 Φ 线性组合，则 ε^p 是 ρ_j^p 的一个 Φ 线性组合；这对 $\varepsilon^{2p}=(\varepsilon^2)^p$，$\varepsilon^{3p}=(\varepsilon^3)^p, \cdots$ 同样成立. 此外因为 ε 是可分的，$\varepsilon \in \Phi(\varepsilon^p)=\Phi[\varepsilon^p]$，于是 ε 本身是 ρ_j^p 的一个 Φ 线性组合. 因为 $[E:\Phi]=q$，故 $(\rho_1^p, \rho_2^p, \cdots, \rho_q^p)$ 是 E/Φ 的一个基，所以 $\{\rho_1^p, \cdots, \rho_n^p\}$ 是 Φ 无关的，而 $\{\rho_1, \cdots, \rho_n\}$ 是 $\Phi^{p^{-1}}$ 无关的. 因为 $\{\rho_1, \cdots, \rho_n\}$ 是 P 的任一有限 Φ 无关子集，这就证明了 P 与 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交.

我们证明以下

定理 10. 若 P 是 Φ 的纯超越扩张，则 P 和 $\Phi^{p^{-1}}$ 在 Φ 上是线性不相交的.

证　设 $P=\Phi(B)$，B 是代数无关集. 已知 P 与 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交当且仅当 B 中元的多项式所成的子代数 $\Phi[B]$ 与 $\Phi^{p^{-1}}$ 线性不相交. 为了证明后者成立，只要找出 $\Phi[B]/\Phi$ 的 $\Phi^{p^{-1}}$ 无关的基就行了. 为此，我们取 $\xi_a \in B$ 的单项式组成的基 M. 显然，如果 m_1 和 m_2 是不同的单项式，则 m_1^p 和 m_2^p 也是不同的单项式，因此 M 的元之 p 次幂的集 M^p 是 Φ 无关集. 因此 M 是 $\Phi^{p^{-1}}$ 无关的. 所以 $\Phi[B]$ 是线性不相交于 $\Phi^{p^{-1}}$ 的，证毕.

现在可以来证明主要定理

麦克莱恩 (Maclane) 准则. 设 P/Φ 是可分生成的（特征为 p），则 P 和 $\Phi^{p^{-1}}$ 在 Φ 上是线性不相交的；反之，若 P 在 Φ 上有限生成，且 P 和 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交，则 P 是 Φ 上可分生成的.

证　首先设 P 在 Φ 上是可分生成的，也就是说 P 在 Φ 上有超越基 B 使得 P 是 $\Sigma=\Phi(B)$ 上可分代数扩张. 由定理 10，Σ 和 $\Phi^{p^{-1}}$ 在 Φ 上是线性不相交的. 由定理 9，P 和 $\Sigma^{p^{-1}}$ 在 Σ 上也是线性不相交的. 因此，P 和 $\Sigma^{p^{-1}}$ 在 Σ 上的子域 $\Sigma(\Phi^{p^{-1}})$ 在 Σ 上是线性不相交的，由引理得到 P 和 $\Phi^{p^{-1}}$ 在 Φ 上是线性不相交的.

其次假设 $P=\Phi(\xi_1, \xi_2, \cdots, \xi_m)$，P 和 $\Phi^{p^{-1}}$ 在 Φ 上是线性不相交的. 不妨设 $\{\xi_1, \xi_2, \cdots, \xi_r\}$ 是一个超越基，而 $\xi_{r+1}, \cdots, \xi_s$ 是 $\Phi(\xi_1, \cdots, \xi_r)$ 上的可分代数元. 如果 $s=m$，则 $\{\xi_1, \cdots, \xi_r\}$ 是可分超越基. 因此假设 ξ_{s+1} 是 $\Sigma=\Phi(\xi_1, \cdots, \xi_r)$ 上的不

可分代数元，$f(x)$ 是 ξ_{s+1} 在Σ上的最小多项式．用 $\xi_1,\cdots,\xi_r$ 的适当的多项式乘 f 得到一个多项式 $F(\xi_1,\cdots,\xi_r,x)\in\Phi[\xi_1,\cdots,\xi_r,x]$，它在 $\Phi[\xi_1,\cdots,\xi_r,x]$ 上是不可约的且满足 $F(\xi_1,\cdots,\xi_r,\xi_{s+1})=0$．因为 f 是不可分多项式，所以它是 x^p 的一个多项式，从而 $F(\xi_1,\cdots,\xi_r,x)$ 是 x^p 的多项式．我们断言，存在一个 $\xi_i(1\leqslant i\leqslant r)$ 使F不是 ξ_i^p 的多项式．否则，在F中实际出现的 $\xi_1,\xi_2,\cdots,\xi_r$，x 的单项式都是 p 次幂的．这就推出

$$F(\xi_1,\cdots,\xi_r,x)=H(\xi_1,\cdots,\xi_r,x)^p$$

在 $\Phi^{p^{-1}}[\xi_1,\cdots,\xi_r,x]$ 中成立．于是 $H(\xi_1,\cdots,\xi_r,\xi_{s+1})=0$，在$H$中出现的 $\xi_1,\cdots,\xi_r,\xi_{s+1}$ 的单项式在 $\Phi^{p^{-1}}$ 上线性相关．因此由P和 $\Phi^{p^{-1}}$ 线性不相交的假设推出这些单项式是 Φ 相关的．由此得到 ξ_{s+1} 是多项式 $h(x)\in\Sigma[x]$ 的根，$h(x)\neq 0$，而次数低于f，这与 f 是 ξ_{s+1} 在Σ上的最小多项式这一事实矛盾．这就表明我们可以假设 $F(\xi_1,\cdots,\xi_r,x)$ 不是 ξ_1^p 的多项式．由关系式 $F(\xi_1,\cdots,\xi_r,\xi_{s+1})=0$ 可见ξ_1 是 $\Phi(\xi_2,\cdots,\xi_r,\xi_{s+1})$ 上的代数元．因为 $\xi_2,\cdots,\xi_r$ 也是这个子域上的代数元．显然 $\{\xi_2,\cdots,\xi_r,\xi_{s+1}\}$ 是一个超越基．

我们来证明 ξ_1 在 $\Sigma'=\Phi(\xi_2,\cdots,\xi_r,\xi_{s+1})$ 上是可分的．已知 $F(\xi_1,\cdots,\xi_r,y)$ 在 $\Phi[\xi_1,\cdots,\xi_r,y]$ 不可约．于是 $F(x,x_2,\cdots,x_r,y)$ 在 $\Phi[x,x_2,\cdots,x_r,y]$ 中不可约，这里 x，x_i，y 是未定元，因此这个多项式在 $\Phi(x_2,\cdots,x_r,y)[x]$ 上不可约，此处 $\Phi(x_2,\cdots,x_r,y)$ 是 $\Phi[x_2,\cdots,x_r,y]$ 的分式域．因为 $\xi_2,\cdots,\xi_r$，ξ_{s+1} 是Φ上的代数无关元，所以在使 $x_i\to\xi_i$ $(2\leqslant i\leqslant r)$，$y\to\xi_{s+1}$ 成立的Φ同构下有 $\Phi(\xi_2,\cdots,\xi_r,\xi_{s+1})\cong\Phi(x_2,\cdots,x_r,y)$．于是 $F(x,\xi_2,\cdots,\xi_r,\xi_{s+1})$ 在 $\Phi(\xi_2,\cdots,\xi_r,\xi_{s+1})[x]$ 中不可约，所以这是ξ_1在Σ'上的最小多项式的倍式．因为这个多项式不是 x^p 的多项式，故ξ_1是Σ'上的可分代数元．因为$\xi_i(1\leqslant i\leqslant s)$ 是 $\Phi(\xi_1,\cdots,\xi_r,\xi_{s+1})$ 上的可分代数元，ξ_1是Σ'上的可分代数元，所以ξ_i是Σ'上的可分代数元．如果将各ξ的下标适当调整，则有超越基 $\xi_1,\cdots,\xi_r$ 使得每个 $\xi_j(1\leqslant j\leqslant s+1)$ 在 $\Phi(\xi_1,$

$\cdots,\xi_r)$ 上是可分代数元. 这就建立了归纳步骤使我们能在生成元 $\xi_1,\cdots,\xi_m$ 中选择 $\xi_1,\cdots,\xi_r$ 使每一 ξ_i 是 $\Sigma=\Phi(\xi_1,\cdots,\xi_r)$ 上的可分代数元. 因此 $\{\xi_1,\cdots,\xi_r\}$ 是 P/Φ 的可分超越基. 从而完全证明了定理的第二部分.

指出下面这一点对将来应用是重要的,即如果$P=\Phi(\xi_1,\cdots,\xi_m)$ 与 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交,我们已经证得可从集 $\{\xi_1,\xi_2,\cdots,\xi_m\}$ 中找出可分超越基. 我们还指出下述的

推论 (F. K. 施米特 (F. K. Schmidt)). 如果 Φ 是完备域, 则任何代数函数域 $\Phi(\xi_1,\cdots,\xi_m)$ 在 Φ 上有可分超越基.

这是麦克莱恩准则的直接结果. 因为 P 确实是线性不相交于 $\Phi^{p^{-1}}=\Phi$ 的.

已经证明的结果,特别是定理 9, 自然使我们可按以下方法推广任意域扩张(不一定是代数的)的可分性概念

定义 3. 域 P 在 Φ 上是可分的,假若其特征为 0, 或特征 $p\neq 0$ 而 P 在 Φ 上线性不相交于 $\Phi^{p^{-1}}$.

定理 9 表明,如果 P 是 Φ 的代数扩张,这就等价于通常的可分性概念. 麦克莱恩准则表明,如果 P 在 Φ 上是有限生成的,则它在 Φ 上可分当且仅当 P 在 Φ 上是可分生成的. 以下定理给出可分性的两个性质. 在代数(扩张)的情况下这是我们所熟悉的.

定理 11. (1) 设 P 在 Φ 上可分, E 是 Φ 上 P 的子域, 则 E 在 Φ 上可分. (2)设 P 在 E 上可分, E 在 Φ 上可分, 则 P 在 Φ 上可分.

证 不妨假设特征 $p\neq 0$. (1) 由 P 和 $\Phi^{p^{-1}}$ 的线性不相交性显然可推出 E 和 $\Phi^{p^{-1}}$ 的线性不相交性. (2) 我们已知 $\Phi^{p^{-1}}$ 在 Φ 上线性不相交于 E, $E^{p^{-1}}$ 在 E 上线性不相交于 P. 则 $E^{p^{-1}}$ 的子域 $E(\Phi^{p^{-1}})$ 在 E 上线性不相交于 P. 利用引理可得 $\Phi^{p^{-1}}$ 和 P 在 Φ 上线性不相交. 所以 P 在 Φ 上是可分的.

我们用两个否定的结果来结束本节的讨论. 首先, 我们已知若 P 在 Φ 上是可分代数的,则 P 在任何中间域上也是可分代数的. 但在一般情形下这是不对的. 如 ξ 是超越元, 在特征 $p\neq 0$ 的情况下 $\Phi(\xi)$ 在 Φ 上可分, 但 $\Phi(\xi)$ 在 $\Phi(\xi^p)$ 上不是可分的. 其

次要注意，一个域可能是在Φ上可分的，但不是可分生成的．下面习题中的第1题给出这样的例子．

习　　题　　30

1．设Φ的特征$p\neq0$，$\mathrm{P}=\Phi(\xi,\xi^{p^{-1}},\xi^{p^{-2}},\cdots)$，这里$\xi$是$\Phi$上的超越元．证明P在$\Phi$上可分但不是可分生成的．

2．设$\Phi_{p^{-m}}$是$\mathrm{P}(\supseteq\Phi)$的代数闭包的子域，由满足$\xi^{p^m}\in\Phi$的元$\xi$组成．令$\Phi^{p^{-\infty}}=\bigcup\Phi^{p^{-m}}$．证明P在$\Phi$上可分当且仅当P和$\Phi^{p^{-\infty}}$在$\Phi$上线性不相交．

3．设E/Φ和Δ/Φ是P/Φ的子域．且E/Φ是纯超越的，而Δ/Φ是代数的．证明E和Δ在Φ上是线性不相交的．

4．令$\mathrm{P}=\Phi(\xi,\eta,\zeta,\tau)$，$\Phi$的特征$p\neq0$，$\xi,\eta,\zeta$是代数无关的且

$$\tau^p=\xi\zeta^p+\eta.$$

证明P在$E=\Phi(\xi,\eta)$上不是可分生成的．

5．(麦克莱恩)设Φ是一个特征$p\neq0$的完全域，P是Φ的一个不完全扩张域且tr.d. $\mathrm{P}/\Phi=1$，证明P在Φ上是可分生成的．

6. 导子　我们知道，引入通常的多项式的形式导数在讨论重根时是很有用的．自$f(x)\to f'(x)$($f(x)$的形式导数)所定义的多项式代数$\Phi[x]$到其自身的映射是在代数$\Phi[x]$中求导的特例．一般来说，考虑一个子代数到代数的求导是比较方便的．下面给出这个在代数中非常重要的一般概念．

定义4.　设$\mathfrak{A}$是代数$\mathfrak{B}$的一个子代数．$\mathfrak{A}$到$\mathfrak{B}$的一个**导子**D是$\mathfrak{A}$到$\mathfrak{B}$内的一个线性映射，满足

$$(ab)D=(aD)b+a(bD)\quad(a,b\in\mathfrak{A}).\tag{8}$$

如果$\mathfrak{A}=\mathfrak{B}$，则称为$\mathfrak{A}$中的**导子**．

我们主要是对代数函数域的导子感兴趣．本节讨论导子的扩张以及关于代数到自身内所有导子组成的代数系的一般结果．我们开始讨论时首先要注意到：研究导子等价于研究某种类型的代数同构，这使我们能够由同态的相应结果得到关于导子的主要性质．为此，引入基域Φ上含基$(1,t)$的代数$\mathfrak{T}$，其中乘法规则为$t^2=0$．因此$\mathfrak{T}=\Phi[x]/(x^2)$，$x$是未定元素，$t$是陪集$x+(x^2)$．如果$\mathfrak{B}$是任意代数，那末我们如下构成代数$\mathfrak{B}\otimes\mathfrak{T}$：如果我们按通常的方法将$\mathfrak{B}$与元$b\otimes1$的子代数等同起来，将$\mathfrak{T}$与元$1\otimes$

$u(u\in\mathfrak{T})$ 的子代数等同起来，那末 $\mathfrak{B}\otimes\mathfrak{T}$ 的元可以唯一地表示为 $b_0+b_1t(b_i\in\mathfrak{B})$ 的形式，t 是 $\mathfrak{T}$ 的生成元素。我们有 $bt=tb$，而且 $\mathfrak{B}\otimes\mathfrak{T}$ 中的一般乘法规则为

$$(b_0+b_1t)(c_0+c_1t)=b_0c_0+(b_0c_1+b_1c_0)t, \tag{9}$$

$b_i,\ c_i\in\mathfrak{B}$。代数 $\mathfrak{B}\otimes\mathfrak{T}$ 叫作 $\mathfrak{B}$ 上的对偶数代数。

现设 D 为 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的导子。可以用它来定义 $\mathfrak{A}$ 到 $\mathfrak{B}\otimes\mathfrak{T}$ 的映射 $s=s(D)$ 如下：

$$a\to a^s\equiv a+(aD)t. \tag{10}$$

显然 s 是线性的。而且当 $a,b\in\mathfrak{A}$ 时有

$$\begin{aligned}a^sb^s&=(a+(aD)t)(b+(bD)t)\\&=ab+(a(bD)+(aD)b)t\\&=ab+((ab)D)t\\&=(ab)^s.\end{aligned}$$

所以 s 是代数 $\mathfrak{A}$ 到对偶数代数 $\mathfrak{B}\otimes\mathfrak{T}$ 内的同态。同态 s 有一个简单的刻划。为此我们引入 $\mathfrak{B}\otimes\mathfrak{T}$ 到 $\mathfrak{B}$ 内的映射

$$\pi:\ a+bt\to a,\quad a,\ b\in\mathfrak{B}.$$

显然，这是 $\mathfrak{B}\otimes\mathfrak{T}$ 到 $\mathfrak{B}$ 内的同态，且在子代数 $\mathfrak{B}$ 上是恒等映射。由此可见，若 $a\in\mathfrak{A}$，s 是由 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的由导子 D 按 (10) 所决定的映射，则 $a^{s\pi}=(a+(aD)t)^\pi=a$。显然这个条件保证了 s 是一个同构。

反之，令 s 是 $\mathfrak{A}$ 到 $\mathfrak{B}\otimes\mathfrak{T}$ 内的同态且 $a^{s\pi}=a$，$a\in\mathfrak{A}$。则

$$a^s=a+bt,$$

$a,\ b\in\mathfrak{B}$，其中 b 是由 a 唯一决定的。因此有映射 $D: a\to b$。因为 $a^s=a+(aD)t$，由 s 的线性性可以得到 D 的线性性。又因为对任意 $a,b\in\mathfrak{A}$ 有 $(ab)^s=a^sb^s$，从而得到

$$\begin{aligned}(a+(aD)t)(b+(bD)t)&=ab+(a(bD)+(aD)b)t\\&=ab+((ab)D)t.\end{aligned}$$

因此 $(ab)D=(aD)b+a(bD)$，D 是一个导子。故有以下结论：

定理 12. 设 $\mathfrak{A}$ 是 $\mathfrak{B}$ 的子代数，D 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的导子，则

$$s:\ a \to a + (aD)t$$

是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 上的对偶数代数 $\mathfrak{B}\otimes\mathfrak{T}$ 内的一个同构，且使 $a^{s\pi} = a$. 反之，$\mathfrak{A}$ 到 $\mathfrak{B}\otimes\mathfrak{T}$ 内的，且满足 $a^{s\pi} = a$ 的任一同态 s 必有形式：$a \to a + (aD)t$. 这里 D 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的导子.

由导子与同构之间的这种联系可以得到一些简单结果.首先，设 $\mathfrak{X}$ 是代数 $\mathfrak{B}$ 中子代数 $\mathfrak{A}$ 的生成元集. D_1 和 D_2 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的两个导子. 假设对每一 $x \in \mathfrak{X}$ 有 $xD_1 = xD_2$, 则 $x^{s_1} = x^{s_2}$. 这里 $s_1 = s(D_1)$, $s_2 = s(D_2)$ 是与 D_1 和 D_2 相连系的 $\mathfrak{A}$ 到 $\mathfrak{B}\otimes\mathfrak{T}$ 内的同构. 于是对每一 $a \in \mathfrak{A}$ 有 $a^{s_1} = a^{s_2}$, 故 $s_1 = s_2$, $D_1 = D_2$. 这就表明，如果两个导子在 $\mathfrak{A}$ 的生成元集上是一致的，则在 $\mathfrak{A}$ 上也是恒同的. 其次要注意，如果 s 是 $\mathfrak{A}$ 到 $\mathfrak{B}\otimes\mathfrak{T}$ 内的同态，且对一切 $x \in \mathfrak{X}$ (生成元集)适合 $x^{s\pi} = x$, 那末对一切 $a \in \mathfrak{A}$ 适合 $a^{s\pi} = a$. 所以 s 按所指出的方式定义了一个导子.

$\mathfrak{A}$ 中满足条件 $cD = 0$ 的元素 c 称为 D **常数**. 显然 c 是 D 常数当且仅当对于同构 $s = s(D)$ 有 $c^s = c$. 由此 (或直接) 可知，D 常数集是 $\mathfrak{A}$ 的子代数. 特别地，1 是对每个导子 D 的 D 常数.如果 $\mathfrak{A}$ 是交换的而 Φ 的特征为 p, 则 $\mathfrak{A}$ 中每一 p 次幂均是 D 常数. 因为在任何交换代数中，由 D 的基本性质 (8) 得到

$$(a^k)D = ka^{k-1}(aD).$$

因此当 $k = p$ 时，有 $(a^p)D = 0$. 我们还要注意，当 $\mathfrak{A} = \mathrm{P}$ 是一个域时，P 的 D 常数集作成 P 的一个子域 Γ. 这是明显的，我们从对 $s = s(D)$ 的考虑或直接由取关系式 $\gamma\gamma^{-1} = 1$ 的导子，就可得到 γ^{-1} 的导子：$\gamma^{-1}D = -(\gamma D)\gamma^{-2}$ 这一法则推出. 如果 $\rho \in \mathrm{P}$, $\gamma \in \Gamma$, 则对于导子 D 有 $(\gamma\rho)D = \gamma(\rho D)$, 这就表明 $D \in \mathfrak{D}_\Gamma(\mathrm{P}, \mathfrak{B})$, 这是 P/Γ 到 $\mathfrak{B}/\Gamma$ 内的导子集. 在考虑域的一个给定导子 D 时，将原来的基域提升为 D 常数所成的域 Γ 或 Γ/Φ 的某个子域 E/Φ 往往是方便的.

现在将导言中推导出来的交换环同态扩张的两个基本结果 I 和 IV′ 搬到导子上来. 我们注意到这些结果对域 Φ 上的代数仍然有效，所以将它们用到这种形式中来. 关于导子扩张的第一个结

果是：

定理 13. 设 P 是 Φ 上的域，$\mathfrak{A}$ 是 P/Φ 的子代数(包含 1)，M 是 $\mathfrak{A}$ 的由非零元(包含 1)组成的乘法封闭子集．令 $\mathfrak{A}_M$ 是 P 中形如 $ab^{-1}(a \in \mathfrak{A},\ b \in M)$ 的元的子代数． D 是 $\mathfrak{A}$ 到 P 内的导子，则 D 有且仅有一种方法扩张为 $\mathfrak{A}_M$ 到 P 内的导子．

证 设 s 是 $\mathfrak{A}$ 到 $P \otimes \mathfrak{T}$ 内的同构：$a \to a + (aD)t$．如果 $a \neq 0$，则 $a^s = a + (aD)t$ 有逆元 $a^{-1} - a^{-2}(aD)t$，因为

$$\begin{aligned}(a + (aD)t)(a^{-1} - a^{-2}(aD)t) \\ = 1 + (aD)a^{-1}t - a^{-1}(aD)t = 1.\end{aligned}$$

由导言中的 I，s 可以扩张为 $\mathfrak{A}_M$ 到 P 内的同构．这个扩张是唯一的且使 $ab^{-1} \to a^s(b^s)^{-1}$．我们有

$$\begin{aligned}a^s(b^s)^{-1} &= (a + (aD)t)(b^{-1} - b^{-2}(bD)t) \\ &= ab^{-1} + ((aD)b^{-1} - ab^{-2}(bD))t.\end{aligned}$$

这个公式表明，如果 s 表示 s 在 $\mathfrak{A}_M$ 的扩张，则

$$(ab^{-1})^{s\pi} = (a^s(b^s)^{-1})^\pi = ab^{-1}.$$

于是 s 决定了 $\mathfrak{A}_M$ 到 P 内的导子

$$ab^{-1} \to (aD)b^{-1} - ab^{-2}(bD). \tag{11}$$

证明过程中还表明了 D 的这个扩张是唯一的．

其次，考虑 P/Φ 的子代数 $\mathfrak{A}$ 以及形为 $\mathfrak{A}[\xi_1, \xi_2, \cdots, \xi_m]$ 的扩张，这里 ξ_i 是域 P 的元．假设给出 $\mathfrak{A}$ 到 P 内的导子 D 以及 P 的元 $\eta_1, \eta_2, \cdots, \eta_m$．我们来寻求关于 D 和 η_i 的条件，以使 D 能扩张为 $\mathfrak{A}[\xi_1, \xi_2, \cdots, \xi_m]$ 的导子 D 且 $\xi_i D = \eta_i\ (i = 1, 2, \cdots, m)$．因为 $\mathfrak{A}$ 和 ξ_i 生成 $\mathfrak{A}[\xi_1, \cdots, \xi_m]$，很明显，如果扩张存在，则它必然唯一．和前面一样，考虑 $\mathfrak{A}$ 到 $P \otimes \mathfrak{T}$ 内的能满足 $a^{s\pi} = a$ 的同构 s：$a \to a + (aD)t$．那么 D 能扩张为 $\mathfrak{A}[\xi_1, \cdots, \xi_m]$ 到 P 内的导子使 $\xi_i \to \eta_i$ 当且仅当 s 能扩张为 $\mathfrak{A}[\xi_1, \cdots, \xi_m]$ 到 $P \otimes \mathfrak{T}$ 内的同构且使 $\xi_i \to \xi_i + \eta_i t$．显然这条件是必要的．如果条件成立，则扩张 s 满足 $a^{s\pi} = a$ 和 $\xi_i^{s\pi} = \xi_i$．象前面那样，s 导出 $\mathfrak{A}[\xi_1, \cdots, \xi_m]$ 的导子．s 的扩张条件已由导言的 IV′ 给出．我们知道满足 $f(\xi_1, \xi_2, \cdots, \xi_m) = 0$ 的多项式

$$f(x_1, x_2, \cdots, x_m) \in \mathfrak{A}[x_1, x_2, \cdots, x_m]$$

(x_i 是未定元) 的集 $\mathfrak{K}$ 是 $\mathfrak{A}[x_1, x_2, \cdots, x_m]$ 的一个理想．关于一个 s 有满足 $\xi_i^s = \xi_i$ ($1 \leqslant i \leqslant m$) 的扩张的条件 IV′ 是 $g^s(\zeta_1, \zeta_2, \cdots, \zeta_m) = 0$，对每个 $g \in \mathfrak{X}$ 成立，这里的 $\mathfrak{X}$ 是 $\mathfrak{K}$ 的生成元集． 因此 D 能扩张为 $\mathfrak{A}[\xi_1, \cdots, \xi_m]$ 到 P 内的导子使 $\xi_i \to \eta_i$ ($i = 1, 2, \cdots, m$) 当且仅当对每一 $g \in \mathfrak{X}$，有

$$g^s(\xi_1 + \eta_1 t, \xi_2 + \eta_2 t, \cdots, \xi_m + \eta_m t) = 0$$

成立．这里 $\mathfrak{X}$ 是使 $f(\xi_1, \cdots, \xi_n) = 0$ 的多项式 $f(x_1, \cdots, x_m) \in \mathfrak{A}[x_1, \cdots, x_m]$ 的理想 $\mathfrak{K}$ 的生成元集．

我们着手详细地找出这些条件．令 $a \in \mathfrak{A}$，考虑单项式

$$M(x_1, \cdots, x_m) = a x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}.$$

则

$$\begin{aligned}
&M^s(\xi_1 + \eta_1 t, \xi_2 + \eta_2 t, \cdots, \xi_m + \eta_m t) \\
&\quad = a^s(\xi_1 + \eta_1 t)^{k_1}(\xi_2 + \eta_2 t)^{k_2} \cdots (\xi_m + \eta_m t)^{k_m} \\
&\quad = (a + (aD)t)(\xi_1 + \eta_1 t)^{k_1}(\xi_2 + \eta_2 t)^{k_2} \cdots (\xi_m \\
&\qquad + \eta_m t)^{k_m} \\
&\quad = a\xi_1^{k_1}\xi_2^{k_2} \cdots \xi_m^{k_m} + (aD)\xi_1^{k_1}\xi_2^{k_2} \cdots \xi_m^{k_m} t \\
&\qquad + (k_1 a \xi_1^{k_1 - 1}\xi_2^{k_2} \cdots \xi_m^{k_m}\eta_1 + k_2 a \xi_1^{k_1}\xi_2^{k_2 - 1}\xi_3^{k_3} \cdots \xi_m^{k_m}\eta_2 \\
&\qquad + \cdots + k_m a \xi_1^{k_1} \cdots \xi_{m-1}^{k_{m-1}}\xi_m^{k_m - 1}\eta_m) t.
\end{aligned}$$

如果定义 $f = \Sigma a_{k_1 \cdots k_m} x_1^{k_1} \cdots x_m^{k_m}$ 关于 x_i 的形式偏导数为

$$\frac{\partial f}{\partial x_i} = \Sigma k_i a_{k_1 \cdots k_m} x_1^{k_1} \cdots x_i^{k_i - 1} \cdots x_m^{k_m}.$$

用 $\left(\dfrac{\partial f}{\partial x_i}\right)_{x_j = \xi_j}$ 表示它在 $(\xi_1, \xi_2, \cdots, \xi_m)$ 的值，则上面的计算表明

$$M^s(\xi_1 + \eta_1 t, \cdots, \xi_m + \eta_m t) = M(\xi_1, \cdots, \xi_m)$$

$$+ \left[M^D(\xi_1, \cdots, \xi_m) + \sum_1^m \left(\frac{\partial M}{\partial x_i}\right)_{x_j = \xi_j} \eta_i \right] t,$$

这里 $f^D(x_1, \cdots, x_m)$ 是将 f 的系数以其在 D 下的象来替代后所得到的多项式．所以，如果 $f \in \mathfrak{A}[x_1, \cdots, x_m]$，那么有

(12) $$f^{t}(\xi_1+\eta_1 t, \xi_2+\eta_2 t, \cdots, \xi_m+\eta_m t)$$
$$= f(\xi_1, \cdots, \xi_m) + f^{D}(\xi_1, \cdots, \xi_m)t$$
$$+ \sum_{1}^{m} \left(\frac{\partial f}{\partial x_i}\right)_{x_j=\xi_j} \eta_i t.$$

显然 $f^{t}(\xi_1+\eta_1 t, \cdots, \xi_m+\eta_m t)=0$ 当且仅当 $f(\xi_1,\cdots,\xi_m)=0$ 以及

(13) $$f^{D}(\xi_1, \cdots, \xi_m) + \sum_{i=1}^{m} \left(\frac{\partial f}{\partial x_i}\right)_{x_j=\xi_j} \eta_i = 0.$$

我们给出准则可以叙述如下

定理 14. 设 $\mathfrak{A}$ 是域 P/Φ 的 Φ 上的子代数，$\xi_1, \xi_2, \cdots, \xi_m$，$\eta_1, \eta_2, \cdots, \eta_m$ 是 P 的元，D 是 $\mathfrak{A}$ 到 P 内的导子. $\mathfrak{K}$ 是由

$$f(\xi_1, \cdots, \xi_m) = 0$$

的多项式 $f(x_1, \cdots, x_m) \in \mathfrak{A}[x_1, \cdots, x_m]$ 所成的理想，$\mathfrak{X}$ 是 $\mathfrak{K}$ 的任意生成元集. 则 D 能扩张为 $\mathfrak{A}[\xi_1, \cdots, \xi_m]$ 到 P 内的导子且使 $\xi_i D = \eta_i\ (i=1, 2, \cdots, m)$ 当且仅当

(14) $$g^{D}(\xi_1, \cdots, \xi_m) + \sum_{i=1}^{m} \left(\frac{\partial g}{\partial x_i}\right)_{x_j=\xi_j} \eta_i = 0$$

对每一 $g \in \mathfrak{X}$ 成立. 如果扩张存在，则它是唯一的.

这个结果的特殊情形如下：如果 ξ_i 是 $\mathfrak{A}$ 上的代数无关元素，则存在 $\mathfrak{A}$ 上导子 D 的扩张将 ξ_i 映到 η_i: $\xi_i \to \eta_i$. 这里 $\eta_1, \cdots, \eta_m$ 是 P 的任意元. 显然，因为此时的理想 $\mathfrak{K}=0$，故扩张的条件总是满足的.

下面考虑一个任意代数 $\mathfrak{B}$，子代数 $\mathfrak{A}$ 以及 $\mathfrak{A}/\Phi$ 到 $\mathfrak{B}/\Phi$ 内的导子的集 $\mathfrak{D}_{\Phi}(\mathfrak{A}, \mathfrak{B})$，如果 $D_1, D_2 \in \mathfrak{D}(\mathfrak{A}, \mathfrak{B})$，而且 $\alpha \in \Phi$，则 αD_1 和 $D_1 + D_2$ 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的线性映射. 此外，如果 $a, b \in \mathfrak{A}$，

$$(ab)(\alpha D_1) = \alpha((ab)D_1) = \alpha((aD_1)b + a(bD_1))$$
$$= (a(\alpha D_1))b + a(b(\alpha D_1))$$
$$(ab)(D_1+D_2) = (ab)D_1 + (ab)D_2$$
$$= (aD_1)b + a(bD_1) + (aD_2)b + a(bD_2)$$

$$= (a(D_1 + D_2))b + a(b(D_1 + D_2)).$$

这就证明了 αD_1 和 $D_1 + D_2$ 也是导子. 因此 $\mathfrak{D}_\Phi(\mathfrak{A},\mathfrak{B})$ 是 $\mathfrak{A}/\Phi$ 到 $\mathfrak{B}/\Phi$ 内线性映射空间 $\mathfrak{D}_\Phi(\mathfrak{A},\mathfrak{B})$ 的子空间. 以下令 c 是 $\mathfrak{B}$ 的中心的元，象往常一样用 c_R 表示 $\mathfrak{B}$ 中的映射 $x \to xc = cx$. 可以断言，如果 D 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的导子，则 D_{c_R} 也是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的导子. 因为 D_{c_R} 显然是线性的. 而且

$$\begin{aligned}(ab)D_{c_R} &= ((aD)b + a(bD))_{c_R} \\ &= (aD_{c_R})b + a((bD)_{c_R}).\end{aligned}$$

故 $D_{c_R} \in \mathfrak{D}(\mathfrak{A},\mathfrak{B})$.

令 $\mathfrak{B} = \mathfrak{A}$, $\mathfrak{D}_\Phi(\mathfrak{A}) = \mathfrak{D}(\mathfrak{A},\mathfrak{A})$ 是 $\mathfrak{A}$ 的导子集. 令 $D_1, D_2 \in \mathfrak{D}_\Phi(\mathfrak{A})$，则 D_1D_2 是空间 $\mathfrak{A}$ 的一个线性变换. 但

$$\begin{aligned}(ab)D_1D_2 &= (a(bD_1) + (aD_1)b)D_2 \\ &= a(bD_1D_2) + (aD_2)(bD_1) + (aD_1)(bD_2) \\ &\quad + (aD_1D_2)b.\end{aligned}$$

因为 $(aD_2)(bD_1) + (aD_1)(bD_2)$ 可以不为 0，故 D_1D_2 不一定是导子，这个“障碍” $(aD_2)(bD_1) + (aD_1)(bD_2)$ 是关于 D_1 和 D_2 对称的，所以对于 D_2D_1 也产生相同的障碍. 如果我们作 $[D_1D_2] = D_1D_2 - D_2D_1$，则这些“障碍”就可消去. 显然就有 $[D_1D_2] \in \mathfrak{D}_\Phi(\mathfrak{A})$. 表示式 $[D_1D_2]$ 叫作 D_1 和 D_2 的**李换位子或加法换位子**. 我们的结果是：$\mathfrak{D}_\Phi(\mathfrak{A})$ 是 $\mathfrak{A}$ 的线性变换空间的子空间，而且在李换位子下封闭，即若 $D_1, D_2 \in \mathfrak{D}_\Phi(\mathfrak{A})$，则 $[D_1D_2] \in \mathfrak{D}_\Phi(\mathfrak{A})$. 具有这一性质的 $\mathfrak{L}_\Phi(\mathfrak{A})$ 的子空间叫作线性变换的**李代数**，李积 $[D_1D_2]$ 是双线性的但不是结合的，它具有基本性质

$$(15)\qquad [DD] = 0,\ [[D_1D_2]D_3] + [[D_2D_3]D_1] + [[D_3D_1]D_2] = 0.$$

第一式是显然的. 第二式直接计算可得，将留给读者去证明. 我们指出以下导子的 k 次幂的莱布尼兹 (Leibniz) 公式：

$$(16)\qquad (ab)D^k = \sum_{i=0}^{k}\binom{k}{i}(aD^i)(bD^{k-i}),\ k = 1, 2, \cdots.$$

对 k 用归纳法是容易证明的．现设基域的特征 $p\neq 0$．则

$$\binom{p}{i}a=0\quad(i=1,2,\cdots,p-1)$$

对任意 $a\in\mathfrak{A}$ 成立．所以在 (16) 中令 $k=p$，就化简为

(17) $$(ab)D^p=(aD^p)b+a(bD^p).$$

故 $\mathfrak{D}_\Phi(\mathfrak{A})$ 在 p 次幂下是封闭的，即若 $D\in\mathfrak{D}_\Phi(\mathfrak{A})$，则 $D^p\in\mathfrak{D}_\Phi(\mathfrak{A})$．在特征 $p\neq 0$ 的域 Φ 上向量空间的线性变换的李代数如果具有这种额外的封闭性，则称为特征为 p 的限制李代数．

习　题　31

1．设 $\mathfrak{A}$ 是 Φ 上的一个代数，$d\in\mathfrak{A}$．验证映射 $a\to[ad]=ad-da$ 是 $\mathfrak{A}$ 的一个导子．这样的导子称为 $\mathfrak{A}$ 的内导子．证明：若 I_d 是由 d 决定的内导子，则

$$I_{\alpha_1d_1+\alpha_2d_2}=\alpha_1I_{d_1}+\alpha_2I_{d_2}\quad(\alpha_i\in\Phi),$$

而且 $I_{[d_1d_2]}=[I_{d_1}I_{d_2}]$．还证明：若 Φ 的特征 $p\neq 0$，则 $I_{d^p}=(I_d)^p$．

2．令 $\mathfrak{A}$ 是代数 $\mathfrak{B}$ 的子代数．验证：$\mathfrak{A}$ 到 $\mathfrak{B}$ 内的映射 D 是一个导子当且仅当 $\mathfrak{A}$ 到矩阵代数 $\mathfrak{B}_2$ 内的映射

$$a\to\begin{pmatrix}a & aD\\ 0 & a\end{pmatrix}$$

是一个同构．这里 $\mathfrak{B}_2$ 是 $\mathfrak{B}$ 上的 2×2 矩阵集．

7．导子，可分性及 p 无关性　我们继续研究域 P/Φ 的导子．首先注意到，如果 $\mathfrak{A}$ 是 P/Φ 的子代数，则 $\mathfrak{A}/\Phi$ 到 P/Φ 的导子 D 可以唯一地扩张为 P 的子域 E 上的导子 D，其中 E 由 $\mathfrak{A}$ 生成，因为 $E=\mathfrak{A}_M$，M 是 $\mathfrak{A}$ 的非零元集，所以这是定理 13 的特殊情形．设 E 是 P/Φ 的子域，D 是 E/Φ 到 P/Φ 内的导子．令 $\xi\in P$，若 ξ 是 P 上的超越元，那么 D 能够扩张到 $E[\xi]$，使 $\xi D=\eta$ 是 P 的任意元素．这是定理 14 的结果．进而，D 能扩张到域 $E(\xi)$ 使 $\xi D=\eta$．次设 ξ 是 E 上的代数元，从而 $E[\xi]=E(\xi)$．令 $f(x)$ 是 ξ 在 E 上的最小多项式，则 $E[x]$ 中使 $h(\xi)=0$ 的多项式 $h(x)$ 组成的理想 $\mathfrak{K}$ 是主理想 $(f(x))$．因此定理 14 表明 D 能扩张为 $E(\xi)$ 的导子且使 $\xi\to\eta$ 当且仅当

(18) $$f^D(\xi)+f'(\xi)\eta=0,$$

$f'(x)$ 是 $f(x)$ 的普通导数(参考导言的V)．如果 ξ 是可分的，则 $f'(\xi)\neq 0$，且由 (18) 给出 $\eta=-f^D(\xi)f'(\xi)^{-1}$． 所以给出$D$的扩张后，$\eta$ 只有一种可能的选择． 可见若 $E(\xi)$ 是E上的可分代数扩张，则 E/Φ 到 P/Φ 内的导子有且仅有一种方法扩张为 $E(\xi)$ 在Φ上的导子．特别是，若在E上有 $D=0$，则D在 $E(\xi)$ 上仅有的扩张导子是 $D=0$．如果 ξ 是不可分的，则 $f'(\xi)=0$．因此D能扩张为 $E(\xi)$ 的导子当且仅当 $f^D(\xi)=0$，而当这一条件被满足时，对任意选定的 $\eta\in P$，D可以扩张到 $E(\xi)$ 上使 $\xi D=\eta$．如果 $f(x)=x^n+\alpha_1x^{n-1}+\cdots$，则

$$f^D(x)=(\alpha_1D)x^{n-1}+(\alpha_2D)x^{n-2}+\cdots.$$

因为 $f(x)$ 是最小多项式，则条件 $f^D(\xi)=0$ 成立当且仅当每一 $\alpha_iD=0$．于是D可扩张到 $E(\xi)$ 上（ξ 是E上的不可分代数元）的充要条件是 ξ 在E上的最小多项式的系数是D常数．特别，在 $f(x)=x^p-\alpha$ 的情形下需要这个判别法． 这时的条件简化为 $\alpha D=0$．

今设 $P=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$ 为Φ的有限生成扩张域(即代数函数域)．$\mathfrak{K}$ 是 $\Phi[x_1,x_2,\cdots,x_m]$ 中使 $f(\xi_1,\xi_2,\cdots,\xi_m)=0$ 的多项式 $f(x_1,x_2,\cdots,x_m)$ 组成的理想，$\mathfrak{X}$ 是 $\mathfrak{K}$ 的基．如果D是代数 $\Phi[\xi_1,\xi_2,\cdots,\xi_m]/\Phi$ 到 P/Φ 内的导子，则D在 P/Φ 上有唯一的扩张．定理 14 (应用于Φ上的导子 $D=0$) 表明：存在一个 $\Phi[\xi_1,\xi_2,\cdots,\xi_m]/\Phi$ 到 P/Φ 内的(从而 P/Φ 到其自身内的)、使 $\xi_iD=\eta_i(i=1,2,\cdots,m)$ 的导子当且仅当

$$\sum_i\left(\frac{\partial g}{\partial x_i}\right)_{x_j=\xi_j}\eta_i=0 \tag{19}$$

对每一 $g\in\mathfrak{X}$ 成立．

在上一节曾提到 P/Φ 的导子集 $\mathfrak{D}_\Phi(P)$．而且看到，当特征 $p\neq 0$ 时这是线性变换的限制李代数，而且 $\mathfrak{D}_\Phi(P)$ 在元 $\rho_R(\rho\in P)$ 右乘下封闭． 所以 $\mathfrak{D}_\Phi(P)$ 是P上右向量空间 $\mathfrak{L}_\Phi(P)$ 的子空间(见 § 1.1)．现将 $\mathfrak{D}_\Phi(P)$ 作为P上右向量空间加以研究，其中 $P=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$．

为此，我们引入m元组$(\rho_1, \rho_2, \cdots, \rho_m)$关于普通加法及P的元的乘法所成的右向量空间$P^{(m)}$，这里$\rho_i \in P$. 如果$D \in \mathfrak{D} = \mathfrak{D}_\Phi(P)$，则把$D$映到元$(\xi_1 D, \xi_2 D, \cdots, \xi_m D) \in P^{(m)}$的映射是P线性的,因而它的象$\mathfrak{D}'$是$P^{(m)}/P$的子空间. 若$\xi_i D = 0 (1 \leqslant i \leqslant m)$，由于$\xi_i$是$P = \Phi(\xi_1, \xi_2, \cdots, \xi_m)$的生成元,故$D = 0$. 这就表明$\mathfrak{D}$到$\mathfrak{D}'$上的映射$D \to (\xi_i D)$的核是0，所以这个映射是$\mathfrak{D}$到$\mathfrak{D}'$上的P线性同构.

以下用前面定义的理想$\mathfrak{R}$的术语描述$P^{(m)}$的子空间$\mathfrak{D}'$. 首先要注意,若$f \in \Phi[x_1, x_2, \cdots, x_m]$，则映射

$$(20) \qquad d_f: (\eta_1, \eta_2, \cdots, \eta_m) \to \sum \left(\frac{\partial f}{\partial x_i}\right)_{x_j = \xi_j} \eta_i.$$

是$P^{(m)}$上的线性函数，即是$P^{(m)}$的共轭空间$P^{(m)*}$中的元. 用$d\mathfrak{X}$表示元dg生成的子空间,其中$g \in \mathfrak{X}$, $\mathfrak{X}$是$\mathfrak{R}$的生成元集. 关于$(\eta_1, \eta_2, \cdots, \eta_m)$的条件(19)也就是$(\eta_i)dg = 0$，对一切$g \in \mathfrak{X}$成立. 因此存在元$D \in \mathfrak{D}_\Phi(P)$使$\xi_i D = \eta_i (1 \leqslant i \leqslant m)$当且仅当$(\eta_i)dg = 0$对一切$g \in \mathfrak{X}$成立. 显然这意味着$\mathfrak{D}'$是$P^{(m)}$中与$P^{(m)*}$的子空间$d\mathfrak{X}$关联的向量的子空间（卷2,中译本p. 51). 我们知道，$\mathfrak{D}'$和$d\mathfrak{X}$的维数之和为m. 如果用完全理想$\mathfrak{R}$代替$\mathfrak{X}$,则有$d\mathfrak{X} \subseteq d\mathfrak{R}$，因为这两个空间有相同的维数$m - [\mathfrak{D}': P]_R$所以$d\mathfrak{X} = d\mathfrak{R}$. 这就证明了对任何两个生成元集，$d\mathfrak{X}$总是相同的,这也是容易直接看出的,我们所得的结果如下:

定理 15. 设$P = \Phi(\xi_1, \xi_2, \cdots, \xi_m)$是$\Phi$上的代数函数域. $\mathfrak{X}$是使$f(\xi_1, \xi_2, \cdots, \xi_m) = 0$成立的多项式$f(x_1, x_2, \cdots, x_m)$所成的理想$\mathfrak{R}$的生成元集，$\mathfrak{D}_\Phi(P)$是$P/\Phi$的导子所成的右P向量空间. 那么

$$(21) \qquad [\mathfrak{D}_\Phi(P): P] = m - [d\mathfrak{X}: P]_R,$$

这里$d\mathfrak{X}$是由(20)所确定的线性函数dg的集，$g \in \mathfrak{X}$.

如果$\mathfrak{X} = \{g_1, g_2, \cdots, g_r\}$，则从$df$的定义及维数与行列式的秩的关系(卷2,中译本p. 20)可知，$[d\mathfrak{X}: P]_R$显然是下列矩阵的秩:

$$(22)\qquad \begin{bmatrix} \left(\frac{\partial g_1}{\partial x_1}\right)_{x_j=\xi_j} & \left(\frac{\partial g_1}{\partial x_2}\right)_{x_j=\xi_j} & \cdots & \left(\frac{\partial g_1}{\partial x_m}\right)_{x_j=\xi_j} \\ \vdots & \vdots & & \vdots \\ \left(\frac{\partial g_r}{\partial x_1}\right)_{x_j=\xi_j} & \left(\frac{\partial g_r}{\partial x_2}\right)_{x_j=\xi_j} & \cdots & \left(\frac{\partial g_r}{\partial x_m}\right)_{x_j=\xi_j} \end{bmatrix}$$

因此，这个“雅可比”矩阵的秩与(21)给出了P上 $\mathfrak{D}_\phi(\mathrm{P})$ 的维数.

我们从 P/Φ 的构造的角度用不同的方法来考察这些问题，首先证明下述的结论

引理 设 $\mathrm{P}=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$，那么0是 P/Φ 到自身内的仅有的导子当且仅当P在Φ上是可分代数的.

证 设ρ是P的可分代数元而D是 P/Φ 的导子，则已知有 $\rho D=0$. 因此当 P/Φ 是可分代数扩张时，则$D=0$是P/Φ 的仅有的导子. 下设P在Φ上不是可分代数的. 不妨令$\{\xi_1,\xi_2,\cdots,\xi_r\}$是超越基(如果P是代数的，则 $r=0$). 若P在$\Phi(\xi_1,\xi_2,\cdots,\xi_r)$上不是可分的，则其特征是 $p\neq 0$. 设Σ是P的子域，由P中在$\Phi(\xi_1,\xi_2,\cdots,\xi_r)$ 上的可分元组成，则$\mathrm{P}\supset\Sigma$且P在Σ上是纯不可分的. 我们断定，存在子域$E\supseteq\Sigma$使 $\mathrm{P}=E(\rho)$，这里ρ在E上的最小多项式是 $x^p-\beta(\beta\in E)$. 我们有 $[\mathrm{P}:\Sigma]<\infty$，可以取$E$为P中包含$\Sigma$的极大真子域，如果 $\sigma\in\mathrm{P}$，$\notin E$，由E的极大性得知 $\mathrm{P}=E(\sigma)$. 因为P在Σ上纯不可分，所以在E上也是纯不可分的. σ在E上的最小多项式形如 $x^{p^k}-\beta(k>0)$. 则

$$\rho=\sigma^{p^{k-1}}\notin E,\ E(\rho)\supset E.$$

由E的极大性得到 $E(\rho)=\mathrm{P}$. 此外，$\rho^p=\sigma^{p^k}=\beta$. 所以 $x^p-\beta$是ρ在E上的最小多项式. 现在已知存在 P/E 的一个导子D使ρD是P的任意元. 若取 $\rho D\neq 0$，D是P/Φ 的一个非零导子. 次设P在 $\Phi(\xi_1,\xi_2,\cdots,\xi_r)$ 上是可分代数的. 但因P在Φ上不是可分代数的，故$r>0$而且存在Φ上 $\Phi[\xi_1,\cdots,\xi_r]$ 到P内的非零导子，它能扩张到P，因此在这种情况下也得到 P/Φ 的非零导子.

可以证明关于 $\mathfrak{D}_\phi(\mathrm{P})$ 在P上维数的以下结果.

定理 16. 如果 $P=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$，则 $[\mathfrak{D}_\Phi(P):P]_R$ 是适合下述条件的最小整数 s：$\{\xi_1,\xi_2,\cdots,\xi_m\}$ 存在子集 $\{\xi_{i_1},\xi_{i_2},\cdots,\xi_{i_s}\}$ 使 P 在 $\Phi(\xi_{i_1},\xi_{i_2},\cdots,\xi_{i_s})$ 上是可分代数的。

证　如前考虑 $\mathfrak{D}=\mathfrak{D}_\Phi(P)$ 到 $P^{(m)}$ 内的映射

$$D\to(\xi_1D,\xi_2D,\cdots,\xi_mD).$$

已知这是到 $P^{(m)}/P$ 内的 P 同构。令 $(D_1,D_2,\cdots,D_s)$ 是 $\mathfrak{D}$ 在 P 上的右基，则 $s\leqslant m$ 且 $\mathfrak{D}$ 在 $P^{(m)}$ 内的象有基 $(\xi_1D_j,\xi_2D_j,\cdots,\xi_mD_j)$，$1\leqslant j\leqslant s$。$s\times m$ 阶矩阵 (ξ_iD_j) 的秩是 s。所以我们能够选择 ξ 的次序使 $\det(\xi_iD_j)\neq0$ $(1\leqslant i,j\leqslant s)$。令 $E=\Phi(\xi_1,\xi_2,\cdots,\xi_s)$，$D$ 是 P/E 到它自身内的导子。则 $D\in\mathfrak{D}$，所以

$$D=\sum_{j=1}^{s}D_j\mu_j,$$

$\mu_j\in P$。且

$$\xi_iD=\sum_{j=1}^{s}(\xi_iD_j)\mu_j=0\qquad(i=1,2,\cdots,s).$$

因为 $\det(\xi_iD_j)\neq0$，这就得到每一 $\mu_j=0$，故 $D=0$，所以 D/E 的仅有的导子是 $D=0$。由引理 P 在 $E=\Phi(\xi_1,\xi_2,\cdots,\xi_s)$ 上是可分代数扩张。设 $\{\xi_{i_1},\xi_{i_2},\cdots,\xi_{i_t}\}$ 是各 ξ 的子集使 P 在 $\Phi(\xi_{i_1},\xi_{i_2},\cdots,\xi_{i_m})$ 上是可分代数的。我们改变 ξ 的次序，不妨设所给集为 $\{\xi_1,\xi_2,\cdots,\xi_t\}$。用这些 ξ 借助于映射 $D\to(\xi_jD)$ $(1\leqslant j\leqslant t)$ 将 $\mathfrak{D}$ 映入 $P^{(t)}$ 内。这还是 P 线性的。若 $(\xi_jD)=0$，则 D 映 $E=\Phi(\xi_1,\xi_2,\cdots,\xi_t)$ 到 0，所以 D 是 P/E 到它自身的导子。因为 P 在 E 上是可分代数的。由引理可知 $D=0$。所以映射 $D\to(\xi_jD)$ 是一个同构，于是 $s=[\mathfrak{D}:P]_R\leqslant t$。证毕。

推论. 如果 $P=\Phi(\xi_1,\xi_2,\cdots,\xi_n)$，则

$$[\mathfrak{D}_\Phi(P):P]_R\geqslant r=\mathrm{tr.d.}P/\Phi,$$

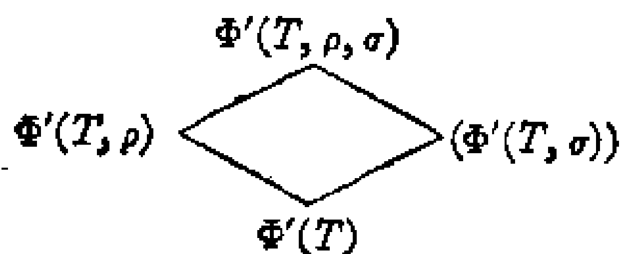
等式成立当且仅当 P 在 Φ 上是可分生成的。

证　定理 16 表明，如果 $s=[\mathfrak{D}:P]_R$，则可以假设 P 在 $E=\Phi(\xi_1,\xi_2,\cdots,\xi_s)$ 上是可分代数的。因为 P 在 E 上是代数的，于是 $\{\xi_1,\xi_2,\cdots,\xi_s\}$ 包含一个超越基，所以 $s\geqslant r$。如果 $s=r$，

由于P在E上可分，则集 $\{\xi_1, \xi_2, \cdots, \xi_r\}$ 是可分超越基．反之，设P是可分生成的,那末可以从ξ的集中选择可分超越基,不妨设它是 $\{\xi_1, \xi_2, \cdots, \xi_r\}$，则P在 $\Phi(\xi_1, \xi_2, \cdots, \xi_r)$ 上是可分代数的．由定理表明 $r \geqslant [\mathfrak{D}:\mathrm{P}]_R$．我们已经证明了 $[\mathfrak{D}:\mathrm{P}]_R \geqslant r$，故 $[\mathfrak{D}:\mathrm{P}]_R = r$．

在本节以下部分我们假设域P的特征是$p \neq 0$．我们会看到，此时导子理论与单纯不可分扩张的研究有紧密联系．假设P在Φ上是纯不可分（代数的）．若 $\rho \in \mathrm{P}$，则ρ在Φ上的最小多项式形如 $x^{p^e} - \beta$（§ 1.9 引理 2)，称e为纯不可分元素ρ的**指数**．显然指数为0当且仅当$\rho \in \Phi$．如果P的元的指数有最大值k，则称P在Φ上的**指数**是k，否则 P/Φ 的指数是无限的．

我们特别感兴趣的是指数 $\leqslant 1$ 的纯不可分扩张． P关于Φ具有这一性质当且仅当 $\mathrm{P}^p \subseteq \Phi$． 这里 P^p 是P的元的p次幂所成子域．如果P是特征为p的Φ的任一扩张,则P在$\Phi' = \Phi(\mathrm{P}^p)$上显然是指数 $\leqslant 1$ 的纯不可分扩张． 我们称元素 $\rho \in \mathrm{P}$ **和P的子集S在Φ上的P中是p相关的**,假若 $\rho \in \Phi'(S)$，其中 $\Phi' = \Phi(\mathrm{P}^p)$．用 $\rho <_p S$ 表示这个关系(在讨论中假定P与Φ是固定的)．我们来证明这就是§ 3 意义下的相关关系．首先,如果$\rho \in S$,则显然有$\rho \in \Phi'(S)$，所以 $\rho <_p S$．如果 $\rho <_p S$，则$\rho \in \Phi'(S)$．因为$\Phi'(S)$是其子域 $\Phi'(F)$ 的并（这里F是S的有限子集)，故对S的某个有限子集F有 $\rho <_p F$． 如果 $\rho \in \Phi'(S)$ 而且每一 $\sigma \in S$ 包含在$\Phi'(T)$ 内,则 $\rho \in \Phi'(T)$． 因此若 $\rho <_p S$，而且每一 $\sigma \in S$ 满足 $\sigma <_p T$，则 $\rho <_p T$．剩下要检验替换公理,就是说,若$\rho \in \Phi'(S)$，而 $\rho \notin \Phi'(S - \{\sigma\})$对$S$的某$\sigma$成立，则 $\sigma \in \Phi'((S - \{\sigma\}) \cup \{\rho\})$．令 $T = S - \{\sigma\}$，并考虑子域$\Phi'(T, \rho, \sigma)$，$\Phi'(T, \rho)$，$\Phi'(T, \sigma)$，$\Phi'(T)$，对此我们有下图:



显然有 $\Phi'(T,\rho)\supseteq\Phi'(T)$, $\Phi'(T,\sigma)\supseteq\Phi'(T)$. 而且 $\rho^p\in\Phi'(T)$ 和 $\sigma^p\in\Phi'(T)$. 于是

$$[\Phi'(T,\sigma):\Phi'(T)]=p=[\Phi'(T,\rho):\Phi'(T)].$$

因为 $\rho\in\Phi'(T,\sigma)$, $\Phi'(T,\rho,\sigma)=\Phi'(T,\sigma)$. 所以 $[\Phi'(T,\rho,\sigma):\Phi'(T)]=p$. 于是 $\Phi'(T,\rho,\sigma)=\Phi'(T,\rho)=\Phi'(T,\sigma)$, 从而 $\sigma<_p T\cup\{\rho\}=(s-\{\sigma\})\cup\{\rho\}$. 这就完全验证了相关关系的公理.

现在可以应用相关关系的一般理论.相应地,称 P 的子集 S 是 p 无关的, 如果 $\sigma\not<_p S-\{\sigma\}$ 对每个 $\sigma\in S$ 成立. 由一般基定理推出: 存在 P 的一个 p 无关子集 B 使每一元素在 B 上是 p 相关的.后一条件等价于 $\mathrm{P}=\Phi'(B)$. 集 B 叫作 P 在 Φ 上的 p 基. 任何两个 p 基有相同的基数.

若 $F=\{\rho_1,\rho_2,\cdots,\rho_m\}$ 是 p 无关集,则 $\rho_i^p=\beta\in\Phi'$. 而且 $\rho_i\notin\Phi'(\rho_1,\rho_2,\cdots,\rho_{i-1})$. 因此 $[\Phi'(\rho_1,\cdots,\rho_i):\Phi'(\rho_1,\cdots,\rho_{i-1})]=p$, $[\Phi'(\rho_1,\cdots,\rho_m):\Phi']=p^m$. 于是 p^m 个元

$$\rho_1^{k_1}\rho_2^{k_2}\cdots\rho_m^{k_m}\quad(0\leqslant k_i<p)\tag{23}$$

构成 $\Phi'(\rho_1,\rho_2,\cdots,\rho_m)$ 在 Φ' 上的一个基. 反之,如果这一条件成立. 则立即得到 F 是 p 无关集. 把这个准则写成下面的等价形式是有用的: F 是 p 无关的当且仅当关系式

$$\Sigma\alpha_{k_1\cdots k_m}\rho_1^{k_1}\cdots\rho_m^{k_m}=0\quad(0\leqslant k<p)\tag{24}$$

(各 $\alpha\in\Phi'$) 只在每一 $\alpha_{k_1\cdots k_m}=0$ 时成立.

我们还要注意任何 p 无关子集 A 能嵌入一个极大 p 无关子集 B 中,而这样的一个集必是一个基.

我们回过来考虑特征为 p 的任意域 P/Φ 的导子. 若 E 是 P/Φ 的子域且 D 是 E/Φ 到 P/Φ 内的一个导子,则对 E 中任何 ε 有 $\varepsilon^pD=p\varepsilon^{p-1}(\varepsilon D)=0$. D 常数集 Γ 是 Φ 上 E 的子域,刚才的注记表明 $\Gamma\supseteq\Phi(E^p)$. 若 $\gamma\in\Gamma$, $\varepsilon\in E$, 则 $(\gamma\varepsilon)D=\gamma(\varepsilon D)$. 就是说 D 是 E/Γ 到 P/Γ 内的导子,因 $\Phi(E^p)\subseteq\Gamma$, 所以 E/Φ 到 P/Φ 内的每一导子也是 $E/\Phi(E^p)$ 到 $\mathrm{P}/\Phi(E^p)$ 的导子,反之亦然. 因此在考虑 E 到 P 内的 Φ 导子时,可以用 $\Phi(E^p)$ 代替 Φ. 所以不

妨假设 $E^p \subseteq \Phi$. 即E在Φ上是指数$\leqslant 1$的纯不可分(扩张).要确定E到P内的Φ导子是容易的. 它由下列定理给出.

定理 17. 设P是特征 $\neq 0$ 的任意域，Φ是子域，E是中间域. 设B是E在Φ上的p基. 令δ是B到P内的任意映射. 则有且仅有一个E到P的Φ导子D使 $\varepsilon D = \delta(\varepsilon)$ 对任意 $\varepsilon \in B$ 成立.

证 如前面所指出的，不失一般性可以假设E在Φ上是指数$\leqslant 1$的纯不可分(扩张). 还可以设$E \supset \Phi$. 这意味着B是非空的，E/Φ 的指数恰好为 1. 令 $\varepsilon \in B$, 集 $B_\varepsilon = B - \{\varepsilon\}$. 则

$$\varepsilon \notin \Phi(B_\varepsilon).$$

所以ε在 $\Phi(B_\varepsilon)$ 上的最小多项式形为 $x^p - \beta$. 因此存在 $E = \Phi(B_\varepsilon, \varepsilon)$ 到 P/Φ 内在 $\Phi(B_\varepsilon)$ 上的导子 D_ε, 使ε映到$\delta(\varepsilon)$. 如果 $F = \{\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_r\}$ 是B的一个有限子集，则 $D_F = D_{\varepsilon_1} + D_{\varepsilon_2} + \cdots + D_{\varepsilon_r}$ 是 E/Φ 到 P/Φ 内的导子. 且使 $\varepsilon_i D_F = \delta(\varepsilon_i)$, $(i=1, 2, \cdots, r)$. 若G是B的包含F的有限子集，则 D_G 在 $\Phi(F)$ 上的限制和 D_F 在 $\Phi(F)$ 上的限制是一致的. 若ξ是E的任一元，则能选择有限子集F使 $\xi \in \Phi(F)$ 且映 $\xi \to \xi D_F$. 显然对任何使 $\xi \in \Phi(F)$ 的有限子集 F, ξD_F 总是相同的. 因此映射 $D: \xi \to \xi D_F$ 是单值的. 立即得到D是 E/Φ 到 P/Φ 内的导子，且使

$$\varepsilon D = \delta(\varepsilon)$$

对每一 $\varepsilon \in B$ 成立. 因为 $E = \Phi(B)$, 故D是唯一的.

令 $\mathfrak{D}_\Phi(E, \mathrm{P})$ 表示 E/Φ 到 P/Φ 内的导子集. 和前面对待 $\mathfrak{D}_\Phi(\mathrm{P})$ 一样(参考 § 1.1 及本书 p.172), 把 $\mathfrak{D}_\Phi(E, \mathrm{P})$看作P上右向量空间. 则有

推论 1. $[\mathfrak{D}_\Phi(E, \mathrm{P}): \mathrm{P}]_R < \infty$, 当且仅当 E/Φ 有一有限p基. 此时 $[\mathfrak{D}_\Phi(E, \mathrm{P}): \mathrm{P}]_R = |B|$.

证 设B是E在Φ上的p基，$\Delta(B, \mathrm{P})$ 是B到P内的映射集，按下面明显的方法把Δ看作P上的右向量空间:

$$(\delta_1 + \delta_2)(\beta) = \delta_1(\beta) + \delta_2(\beta), \ (\delta_i \in \Delta, \beta \in B),$$

$$(\delta_\rho)(\beta) = \delta(\beta)\rho, \ (\delta \in \Delta, \beta \in B, \rho \in \mathrm{P}).$$

作 $\mathfrak{D}_\Phi(E, \mathrm{P})$ 到 $\Delta(B, \mathrm{P})$ 内的映射，它将 $D \in \mathfrak{D}_\Phi(E, \mathrm{P})$ 映到

它在B上的限制δ. 这个映射是线性的. 因为 $E=\Phi(B)$, 所以 $D\rightarrow\delta$ 是一个同构. 此外定理表明映射是满射. 现在如果B是无限的,则 $[\Delta(B,\mathrm{P}):\mathrm{P}]_R$ 也是无限的(甚至是不可数的). 如果B是有限的,就是说 $B=\{\beta_1,\beta_2,\cdots,\beta_r\}$, 则满足 $\delta_i(\beta_j)=\delta_{ij}$ (克罗内克 δ_{ij}) 的 r 个映射 δ_i 形成一个基. 所以

$$r=[\Delta(B,\mathrm{P}):\mathrm{P}]_R=[\mathfrak{D}_\Phi(E,\mathrm{P}):\mathrm{P}]_R.$$

在 $\mathrm{P}=E=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$ 特殊情况下,除了定理 15 与定理 16 外,这个推论给出了当特征 $p\neq 0$ 时计算 $[\mathfrak{D}_\Phi(\mathrm{P}):\mathrm{P}]_R$ 的第三种方法,即这个维数等于 P/Φ 的 p 基中的元素数. 定理 17 的第二个推论如下

推论 2. E/Φ 到 P/Φ 内的每一导子能扩张到 P/Φ 上当且仅当 E/Φ 的任何p基B的元在 P/Φ 内是p无关的.

证 如果条件成立, 则B能嵌入P在Φ上的p基C. 若D是 E/Φ 到 P/Φ 的导子,则D在B上的限制δ_B能扩张为C到P的映射δ_C. P/Φ到自身内的对应的导子D'是D的扩张. 另外,假设B在Φ上的P内不是p无关的, β是B的元,在P中和 $B_\beta=B-\{\beta\}$ 是p相关的. 若D'是P的满足 $\beta'D'=0$ (对一切 $\beta'\in B_\beta$) 的任一导子, 则因 $\beta\in\Phi(\mathrm{P}^p,B_\beta)$ 而有 $\beta D'=0$. 定理表明存在E到P内的导子D使 $\beta'D=0(\beta'\in B_\beta)$ 但 $\beta D\neq 0$. 显然, 这样的导子不能扩张到P.

下面两个推论处理$E=\mathrm{P}$的特殊情形. 证明与刚才给出的十分类似,留作习题.

推论 3. 设P是Φ上特征$p\neq 0$的任意域. 则元 $\rho(\in\mathrm{P})$ 属于 $\Phi'=\Phi(\mathrm{P}^p)$ 当且仅当P在Φ上的每一导子D有 $\rho D=0$.

推论 4. P的子集S是p无关的当且仅当对每一 $\rho\in S$, 存在P在Φ上的导子D使 $\rho D\neq 0$, 而对每一S中的$\sigma\neq\rho$有

$$\sigma D=0.$$

现在取Φ为素域 $\Phi_0(\cong I_p)$ 而将所得结果特殊化: E/Φ_0 到 P/Φ_0 内的导子简称为E**到**P**内的导子**. 我们注意到若D是E到P内的映射且满足 $(\varepsilon_1+\varepsilon_2)D=\varepsilon_1 D+\varepsilon_2 D$ 及

$$(\varepsilon_1\varepsilon_2)D=(\varepsilon_1D)\varepsilon_2+\varepsilon_1(\varepsilon_2D),$$

那末D是现在意义下的E到P内的导子．这是因为

$$(\alpha\varepsilon)D=\alpha(\varepsilon D)\ \ (\alpha\in\Phi_0)$$

是第一个性质的结果．我们还有 $\Phi_0(E^p)=E^p$． 因此推论 3 给出了一个元为p次幂的判定方法．现在研究推论 2 中给出的E到P内的导子能扩张为P的导子的判别方法．我们要证明所给条件等价于P在E上的可分性(在一般意义下).首先假设条件为E(在Φ_0上)的每个p基在P中是p无关的．令 $\rho_1,\rho_2,\cdots,\rho_n\in$ P，且设$\Sigma\varepsilon_i\rho_i^p=0$ 其中 $\varepsilon_i(\neq0)\in E$．如果$B$是$E$的一个$p$基，则可以写成 $\varepsilon_i=\Sigma\gamma_{ik_1k_2\cdots k_r}\beta_1^{k_1}\beta_2^{k_2}\cdots\beta_r^{k_r}$，其中 $\beta_j\in B$，$0\leqslant k_a<p$，$\gamma_{ik_1\cdots k_r}\in E^p$．于是有 $\Sigma\delta_{k\cdots k_r}\beta_1^{k_1}\cdots\beta_r^{k_r}=0$，这里

$$\delta_{k_1\cdots k_r}=\sum_i\gamma_{ik_1\cdots k_r}\rho_i^p\in \mathrm{P}^p.$$

因为这些β在P中是p无关的，故 $\delta_{k_1\cdots k_r}=0$，设 $\gamma_{ik_1\cdots k_r}=\eta_{ik\cdots k_r}^p$ ($\eta_{ik_1\cdots k_r}\in E$)，则由 $0=\delta_{k_1\cdots k_r}=\sum\limits_i\eta_{ik_1\cdots k_r}^p\rho_i^p$ 给出

$$\sum_i\eta_{ik_1\cdots k_r}\rho_i=0$$

对一切k_i成立．因为 $\varepsilon_i\neq0$ 这些关系中有一个是非平凡的，故我们已经证明了对任何形为 $\Sigma\varepsilon_i\rho_i^p=0(\varepsilon_i\in E,\rho_i\in \mathrm{P})$的非平凡关系可以推出一个非平凡关系 $\Sigma\eta_i\rho_i=0\ (\eta_i\in E)$． 这就等价于 P$/E$ 的可分性．相反地，设P在E上是可分的，令 $\beta_1,\beta_2,\cdots,\beta_r$ 是E的元，且有关系式 $\Sigma\gamma_{k_1\cdots k_r}\beta_1^{k_1}\beta_2^{k_2}\cdots\beta_r^{k_r}=0$，$\gamma_{k_1\cdots k_r}=\eta_{k_1\cdots k_r}^p\in \mathrm{P}^p$，$(0\leqslant k_i<p)$．令 $\{\rho_\alpha\}$ 是P$/E$的一个基，且

$$\eta_{k_1\cdots k_r}=\sum_{i=1}^n\lambda_{k_1\cdots k_ri}\rho_i\ \ (\text{各}\ \lambda\in E),$$

则有

$$0=\Sigma\gamma_{k_1\cdots k_r}\beta_1^{k_1}\cdots\beta_r^{k_r}=\sum_i\mu_i\rho_i^p,$$

这里 $\mu_i=\sum\limits_k\lambda_{k_1\cdots k_ri}^p\beta_1^{k_1}\beta_2^{k_2}\cdots\beta_r^{k_r}$，因为P在$E$上可分，由$\Sigma\mu_i\rho_i^p=0$可推出每个 $\mu_i=0$．所以

$$\sum \lambda_{k_1\cdots k_r i}^p \beta_1^{k_1}\beta_2^{k_2}\cdots\beta_r^{k_r}=0 \quad (i=1,2,\cdots,n).$$

如果有某个 $\gamma_{k_1\cdots k_r}\neq 0$ 那么有某个 $\lambda_{k_1\cdots k_r i}\neq 0$，从而我们得到了一个系数在 E^p 内关于幂 $\beta_1^{k_1}\cdots\beta_r^{k_r}$ 的、非平凡关系式。由此推得：若 $\{\beta_1,\beta_2,\cdots,\beta_r\}$ 在P中是 p 相关的，则它在 E 中也是 p 相关的。显然这就得到推论 2 的条件，因此推论 2 给出以下

定理 18. 在特征为 p 的域 P/E 中，以下两个条件是等价的：(1) P/E 是可分的，(2) E 到P内的每一导子可以扩张为P的导子。

习 题 32

1. 设 $\mathrm{P}=\Phi(\rho)$，这里 $\rho^{p^2}\in\Phi$ 但 $\rho^p\notin\Phi$。证明 $\{\rho^p\}$ 是 $E=\Phi(\rho^p)/\Phi$ 的 p 无关子集，但不是 P/Φ 的 p 无关子集。

2. 设 B 是特征 $p\neq 0$ 的域P在 Φ 上的 p 基。证明：对每一正整数 k，$\mathrm{P}=\Phi(\mathrm{P}^{p^k},B)$。

在习题的第 3，4 两题中，P是 Φ 上指数为 1 的纯不可分扩张，而且 $[\mathrm{P}:\Phi]=p^m<\infty$。

3. (贝尔 (Baer)) 证明：存在 P/Φ 的导子 D 使 D 常数只能是 Φ 的元(提示：令 E 是P的真子域，假设 E/Φ 有满足条件的导子 D. 设 $\rho\in\mathrm{P}$，$\notin E$，可以选择 $\beta\in E$，但不是 εD 的形式 $(\varepsilon\in E)$。将 D 扩张到 $E(\rho)$ 使 $\rho D=\beta$。则 $E(\rho)$ 的 D 常数只能是 Φ 的元)。

4. 证明可以选择第 3 题中的 D 是幂零的。

5. (弗斯 (Faith)) 设P是 Φ 上的代数函数域(任意特征)，E 是 Φ 上的子域。证明 $[\mathfrak{D}_\Phi(\mathrm{P}):\mathrm{P}]_R\geqslant[\mathfrak{D}_\Phi(E):E]_R$。

6. 设 $\mathrm{P}=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$，$\Phi$ 的特征 $p\neq 0$，证明 $\mathrm{tr.d.P}/\Phi$ 不超过 P/Φ 的 p 基的元数。

7. 设P与 Φ 如第 6 题。证明：若 $(D_1,D_2,\cdots,D_r)$ 是 $\mathfrak{D}_\Phi(\mathrm{P})$ 的右P基，则元 $\rho_1,\rho_2,\cdots,\rho_r$ 形成P在 Φ 上的一个 p 基当且仅当矩阵 $(\rho_i D_j)$ 是非奇异的。并证明：若 $\rho_1,\rho_2,\cdots,\rho_r$ 是一个 p 基，则元 $D_1,D_2,\cdots,D_r$ 形成 $\mathfrak{D}_\Phi(\mathrm{P})$ 的一个右P基当且仅当 $(\rho_i D_j)$ 是非奇异的。

8. 设 $\mathrm{P}=\Phi(\xi_1,\xi_2,\cdots,\xi_m)$，证明 P/Φ 是可分代数扩张域当且仅当在 $\Phi[x_1,x_2,\cdots,x_m]$ 中存在 m 个多项式 $g_1(x_1,x_2,\cdots,x_m),\cdots,g_m(x_1,x_2,\cdots,x_m)$ 使

$$g_i(\xi_1,\xi_2,\cdots,\xi_m)=0$$

及雅可比行列式

$$\det\left(\left(\frac{\partial g_i}{\partial x_j}\right)_{x_k=\xi_k}\right)\neq 0.$$

9. 设 D 是 P/Φ 的一个导子，Γ 是 D 常数子域。证明元 $\rho_1,\rho_2,\cdots,\rho_m$ 是 Γ 相关

的当且仅当朗斯基 (Wronskian) 行列式

$$\begin{vmatrix} \rho_1 & \rho_2 & \cdots & \rho_m \\ \rho_1 D & \rho_2 D & \cdots & \rho_m D \\ \vdots & \vdots & \cdots & \vdots \\ \rho_1 D^{m-1} & \rho_2 D^{m-1} & \cdots & \rho_m D^{m-1} \end{vmatrix} = 0.$$

8. 指数为 1 的纯不可分扩张的伽罗瓦理论 本节讲述指数为 1 的纯不可分扩张的伽罗瓦理论. 这里用导子的李代数来代替经典理论中伽罗瓦群的作用.

首先,设 P 是 Φ 上指数 $\leqslant 1$ 的纯不可分扩张,且在 Φ 上有有限 p 基 $B=\{\rho_1, \rho_2, \cdots, \rho_m\}$, 那末 $[P:\Phi]=p^m$. 而元 $\rho_1^{k_1}\rho_2^{k_2}\cdots\rho_m^{k_m}$ $(0\leqslant k_i<p)$ 形成 P/Φ 的一个基. 我们有 $\rho_i^p=\beta_i\in\Phi$. 和前面一样, 用 $\mathfrak{D}_\Phi(P)$ 表示 P/Φ 的导子集. 我们知道 $\mathfrak{D}_\Phi(P)$ 是 P 在 Φ 上线性变换的限制李代数. 这就是说 $\mathfrak{D}_\Phi(P)$ 是 Φ 上向量空间 P 的线性变换空间 $\mathfrak{L}_\Phi(P)$ 的一个子空间,它满足:若 $D_1, D_2\in\mathfrak{D}_\Phi(P)$, 则 $[D_1D_2]=D_1D_2-D_2D_1\in\mathfrak{D}_\Phi(P)$, 而且 $D_1^p\in\mathfrak{D}_\Phi(P)$. 我们还看到 $\mathfrak{D}_\Phi(P)$ 是 P 上关于 $D_\rho=D_{\rho_R}(\rho\in P)$ 的右向量空间, 而且知道 $[\mathfrak{D}_\Phi(P):P]_R=m$ (定理 17 的推论 1) 以及: 若 ρ 是 P 中对一切 $D\in\mathfrak{D}_\Phi(P)$满足 $\rho D=0$ 的元,则 $\rho\in\Phi$ (定理 17 推论 3). 这最后一个结论给出了我们要建立的伽罗瓦对应的一半.

为了得到这个对应的另一半, 我们假设 P 是特征 $p\neq 0$ 的任意域,不指定任何域作为基域. 上节最后讨论过 P 的导子,它可定义为 P 在其素域上的导子或者定义为 (P, +) 的适合条件

$$(\rho\sigma)D=(\rho D)\sigma+\rho(\sigma D)\ \ (\rho, \sigma\in P)$$

的自同态.设已给定一个 P 的导子的集 $\mathfrak{D}$ 符合以下闭包性质: (1) $\mathfrak{D}$ 关于加法封闭. (2) $\mathfrak{D}$ 关于李换位子 $[D_1D_2]$ 封闭. (3) $\mathfrak{D}$ 关于 p 次幂封闭. (4) $\mathfrak{D}$ 关于用元 $\rho_R(\rho\in P)$ 右乘封闭.条件 (1) 和 (4) 总起来说是: $\mathfrak{D}$ 是加群 (P, +) 的自同态所成右向量空间的子空间. 它被看作 P 上关于运算 $A_\rho=A_{R_\rho}$ 的空间.(P, +)的满足(1)到 (4) 的任何自同态集叫作 (P, +) 的自同态的一个限制 P 李

代数[1]．现在我们可以建立以下定理：

定理 19（贾柯勃逊） 设 P 是特征 $p \neq 0$ 的域，$\mathfrak{D}$ 是 P 中导子的限制 P 李代数，且满足 $[\mathfrak{D}:P]_R = m < \infty$．那末：(1) 若 Φ 是 $\mathfrak{D}$ 常数所成的子域，则 P 是 Φ 上指数 $\leqslant 1$ 的纯不可分扩张．且 $[P:\Phi] = p^m$．(2) 若 D 是 P 在 Φ 上的任一导子，则 $D \in \mathfrak{D}$．(3) 若 $(D_1, D_2, \cdots, D_m)$ 是 $\mathfrak{D}$ 在 P 上的任一右基，则下列单项式的集

(25) $$D_1^{k_1} D_2^{k_2} \cdots D_m^{k_m}, \quad 0 \leqslant k_i < p \ (D_i^0 = 1)$$

是 P 在 Φ 上的线性变换环 $\mathfrak{L}_\Phi(P)$ 的一个右基（$\mathfrak{L}_\Phi(P)$ 看作 P 上右向量空间）．

证 证明思路与自同构的伽罗瓦理论中所用方法基本相同：用所给集 $\mathfrak{D}$ 定义一个满足贾柯勃逊-布尔巴基定理（定理 1.2）假设的自同态集 $\mathfrak{A}$，今设 $\mathfrak{A}$ 是 (25) 给出的自同态的右 P 线性组合的集，显然 $\mathfrak{A}$ 是 P 上的右向量空间，而且 $[\mathfrak{A}:P]_R < \infty$．剩下要证明 $\mathfrak{A}$ 是 (P, +) 的自同态环的子环．为此只须证明 $1 \in \mathfrak{A}$ 且 $\mathfrak{A}$ 关于乘法封闭就够了．因为 $\mathfrak{A}$ 含有 $D_1^0 D_2^0 \cdots D_m^0 = 1$，故 $1 \in \mathfrak{A}$ 是明显的．为了证明乘法封闭性，只要证明每个积 $(D_1^{k_1} D_2^{k_2} \cdots D_m^{k_m}) D_j \in \mathfrak{A}$ $(\rho \in P)$ 就够了．因为如果这是成立的，则每个乘积 $(D_1^{k_1} \cdots D_m^{k_m} \rho)(D_1^{l_1} \cdots D_m^{l_m} \sigma)$ 含于 $\mathfrak{A}$ 中 $(\sigma \in P)$．设 D 是 P 的导子，则条件

$$(\xi\rho)D = (\xi D)\rho + \xi(\rho D)$$

能写成算子形式：

(26) $$\rho_R D = D \rho_R + (\rho D)_R.$$

这就得出 $(D_1^{k_1} \cdots D_m^{k_m} \rho) D_j = D_1^{k_1} \cdots D_m^{k_m} D_j \rho + D_1^{k_1} \cdots D_m^{k_m} (\rho D_j)$．因此只要证明了 $D_1^{k_1} \cdots D_m^{k_m} D_j \in \mathfrak{A}$ $(j = 1, \cdots, m$ 及 $0 \leqslant k_i \leqslant p-1)$，就得到 $\mathfrak{A}$ 关于乘法的封闭性．我们规定单项式 $D_1^{k_1} D_2^{k_2} \cdots D_m^{k_m}$ 的（显然的）次数为 $N = k_1 + k_2 + \cdots + k_m$．我们要证明 $D_1^{k_1} \cdots D_m^{k_m} D_j$ 是 (25) 中次数 $\leqslant N+1$ 的单项式的右 P 线性组合．如果 $N = 0$，这是显然的．假设对于次数 $\Sigma l_i < N$ 的每一 $D_1^{l_1} \cdots$

---

1) 这个术语并不意味着 $\mathfrak{D}$ 是基域 P 上的代数．对于一个代数条件之一是

$$[D_1 D_2]_\rho = [D_1 \rho, D_2] = [D_1, D_2 \rho],$$

但元对任意 ρ 并不一定成立（见下面的 (26) 式）．——著者注．

$D_m^{k_m}$ 结论成立. 先设 $j=m$. 那末如果 $k_m<p-1$, $D_1^{k_1}\cdots D_m^{k_m}D_m$ 就是 (25) 中某一个次数为 $N+1$ 的单项式,因此在此情况下结论成立. 如果 $k_m=p-1$, 则

$$(D_1^{k_1}\cdots D_m^{k_m})D_m=D_1^{k_1}\cdots D_{m-1}^{k_{m-1}}D_m^p.$$

因为 D 关于 p 次幂封闭,故 $D_m^p=\Sigma D_i\mu_{im}$, 所以

$$D_1^{k_1}\cdots D_m^{k_m}D_m=\Sigma D_1^{k_1}\cdots D_{m-1}^{k_{m-1}}D_i\mu_{im}.$$

由归纳假设得到 $D_1^{k_1}\cdots D_m^{k_m}D_m$ 是 (25) 中次数 $\leqslant N+1$ 的单项式的一个右 P 线性组合. 这就得到了 $j=m$ 时的结果, 所以我们可作一附加的归纳假设: 设对一切 $l>j$ 关于 $D_1^{k_1}\cdots D_m^{k_m}D_l$ 的论断成立. 因为 $N=\Sigma k_i>0$. 所以有某些 $k_i\neq 0$, 不妨设 $k_r\neq 0$, 且当 $s>r$ 时有 $k_s=0$. 则有 $(D_1^{k_1}\cdots D_m^{k_m})D_j=(D_1^{k_1}\cdots D_r^{k_r})D_j$. 如果 $j>r$, 这个积就是单项式 (25), 所以此时结论成立. 如果 $j=r$, 则可用前面 $j=m$ 时的论证来证明结论. 剩下要考虑 $j<r$ 的情形. 因为 $\mathfrak{D}$ 关于换位封闭,

$$D_rD_j=D_jD_r+\Sigma D_h\nu_{hrj},\quad \nu_{hrj}\in \mathrm{P},$$

则

$$D_1^{k_1}\cdots D_r^{k_r}D_j=D_1^{k_1}\cdots D_r^{k_r-1}D_jD_r$$
$$+\sum_h D_1^{k_1}\cdots D_r^{k_r-1}D_h\nu_{hjr},$$

而每个 $D_1^{k_1}\cdots D_r^{k_r-1}D_h$ 是总次数 $<N$的单项式 (25) 的一个 P 线性组合. 这对 $D_1^{k_1}\cdots D_r^{k_r-1}D_j$ 也是成立的,因为 $r>j$ 右乘以 D_r 成为总次数 $\leqslant N+1$ 的项 (25) 的 P 线性组合. 这就完全证明了我们的断言, 而且表明 $\mathfrak{A}$ 是 (P, +) 的自同态环的子环. 从 $\mathfrak{A}$ 的定义易见 $[\mathfrak{A}:\mathrm{P}]_R\leqslant p^m$, 其等式成立当且仅当单项式 (25) 是右 P 无关的, 从而是一个基. 现在把贾柯勃逊-布尔巴基定理(定理 1.2)用到$\mathfrak{A}$上得到以下结论:若 Φ 是 P 中满足 $\alpha_R A=A\alpha_R$ (对一切 $A\in\mathfrak{A}$) 的元 α 所成的子域,则 $[\mathrm{P}:\Phi]=[\mathfrak{A}:\mathrm{P}]_R$ 而且

$$\mathfrak{A}=\mathfrak{L}_\Phi(\mathrm{P}).$$

显然 $\alpha_R A=A\alpha_R$ 对一切 $A\in\mathfrak{A}$ 成立当且仅当 $\alpha_R D=D\alpha_R$ 对一切 $D\in\mathfrak{D}$ 成立. 因为 $\alpha_R D=D\alpha_R+(\alpha D)_R$, 所以这个条件也就

是对一切 $D\in\mathfrak{D}$ 有 $\alpha D=0$ 成立。于是我们看到 Φ 是 $\mathfrak{D}$ 常数所成子域。如果 ρ 是 P 的任意元，则 ρ^p 是 $\mathfrak{D}$ 常数。因为 P 是 Φ 上指数 $\leqslant 1$ 的纯不可分(扩张)，所以有 $[\mathrm{P}:\Phi]=p^{m'}$，这里 m' 是 P/Φ 的 p 基的元数。因为 $[\mathrm{P}:\Phi]=[\mathfrak{A}:\mathrm{P}]_R\leqslant p^m$，故 $m'\leqslant m$。此外还知道，若 $\mathfrak{D}_\Phi(\mathrm{P})$ 是 P/Φ 的导子集，则 $[\mathfrak{D}_\Phi(\mathrm{P}):\mathrm{P}]_R=m'$。如果 $\alpha\in\Phi$ 且 $D\in\mathfrak{D}$，则 $(\alpha\rho)D=\alpha(\rho D)+(\alpha D)_\rho=\alpha(\rho D)$，故 $D\in\mathfrak{D}_\Phi(\mathrm{P})$，于是 $\mathfrak{D}\subseteq\mathfrak{D}_\Phi(\mathrm{P})$。又因为 $[\mathfrak{D}:\mathrm{P}]_R=m$，我们有 $\mathfrak{D}=\mathfrak{D}_\Phi(\mathrm{P})$ 且 $m=m'$。那末 $\mathfrak{D}$ 包含 P/Φ 的每一导子，$[\mathrm{P}:\Phi]=p^m$，证毕。

现在可以建立由特征为 p 的任意域 P 所决定的下面两个集族之间的伽罗瓦型对应：令 $\mathscr{F}$ 是 P 的子域 Φ 的集族，且使 P 是 Φ 上指数 $\leqslant 1$ 的纯不可分(扩张)，$[\mathrm{P}:\Phi]<\infty$。令 $\mathscr{D}$ 表示 P 中导子代数 $\mathfrak{D}$ 的类，它是 P 上有限维限制 P 李代数。如果 $\mathfrak{D}\in\mathscr{D}$，令 $C(\mathfrak{D})$ 是 $\mathfrak{D}$ 常数所成的子域。如果 $\Phi\in\mathscr{F}$，令 $\mathfrak{D}_\Phi(\mathrm{P})$ 是 P/Φ 的导子集。则 $C(\mathfrak{D}_\Phi(\mathrm{P}))=\Phi$，而且 $\mathfrak{D}_{C(\mathfrak{D})}(C(\mathfrak{D}))=\mathfrak{D}$，特别是我们得到 P/Φ 的中间域 (P 是 Φ 上的指数 $\leqslant 1$ 的纯不可分的扩张域，且 $[\mathrm{P}:\Phi]<\infty$) 和李代数 $\mathfrak{D}_\Phi(\mathrm{P})$ 的限制 P 李子代数之间的 1-1 对应。

习　题　33

1. 设 $\Phi[x,y]$ 是特征为 p 的域上未定元 x,y 的多项式环，$\mathfrak{A}$ 是 Φ 上的任意代数。利用 $\Phi[x,y]$ 中的恒等式 $(x-y)^p=x^p-y^p$ 和 $(x-y)^{p-1}=\sum_{i+j=p-1}x^iy^j$ 证明 $\mathfrak{A}$ 中的恒等式：

$$[\cdots\overbrace{[ba]a]\cdots a}^{p}]=[ba^p]. \tag{27}$$

$$[\cdots\overbrace{[ba]a]\cdots a}^{p-1}]=\sum_{i+j=p-1}a^iba^j. \tag{28}$$

(提示：注意 $[ba]=b(a_R-a_L)$，a_R 与 a_L 是由 $\mathfrak{A}$ 中元 a 决定的右乘和左乘(运算)。在 a_R 与 a_L 生成的线性变换的交换代数中取 $x=a_R$，$y=a_L$ 得到所给恒等式的特殊情形)。

2. 设 $\mathfrak{A}$ 如第 1 题，$\mathfrak{A}[x]$ 是 $\mathfrak{A}$ 上未定元 x 的多项式代数，设 $a,b\in\mathfrak{A}$，而且写出

(29) $$(a+bx)^p = a^p + \sum_1^{p-1} s_i(a, b)x^i + b^p x^p.$$

根据 $\Sigma a_i x^i \to \Sigma i a_i x^{i-1}$ 是 $\mathfrak{A}[x]$ 中的导子这一事实及 (29) 得到

(30) $$\sum_{i+j=p-1} (a+bx)^i b (a+bx)^j = \sum_{i=1}^{p-1} i s_i(a, b) x^{i-1}.$$

用这一关系式及 (28) 证明以下恒等式

(31) $$(a+b)^p = a^p + b^p + \sum_1^{p-1} s_i(a, b),$$

这里 $i s_i(a, b)$ 是

$$[\cdots[[b, a+bx]\overbrace{a+bx]\cdots a+bx}^{p-1}]$$

中 x^{i-1} 的系数.

3. 设 $P = \Phi(\rho_1, \cdots, \rho_m)$, Φ 的特征 $p \neq 0$, $\rho_i^p = \beta_i \in \Phi$, $[P:\Phi] = p^m$. 令 D 是 P/Φ 的导子使 Φ 是 D 常数子域(见 § 7 习题中的第 3 题). 证明: D 作为 P 在 Φ 上的线性变换其最小多项式是形为

(32) $$x^{p^m} + \beta_1 x^{p^{m-1}} + \beta_2 x^{p^{m-2}} + \cdots + \beta_m x, \ \beta_i \in \Phi$$

的 p 多项式. 并证明存在元 $\rho \in P$ 使 $(\rho, \rho D, \cdots, \rho D^{p^m-1})$ 是 P 在 Φ 上的一个基(这与关于可分正规扩张的正规基定理类似). 再证明 P 在 Φ 上的线性变换代数 $\mathfrak{L}_\Phi(P)$ 中每一元能且只能用一种方法写成

(33) $$1\sigma_0 + D\sigma_1 + D^2\sigma_2 + \cdots + D^{p^m-1}\sigma_{p^m-1}, \ \sigma_i \in P$$

的形式.

4. 设 P, Φ 如第 3 题. $\mathfrak{D}_\Phi(P)$ 是 P/Φ 的导子集,设 $\mathfrak{J}$ 是 P 中右向量空间 $\mathfrak{D}_\Phi(P)$ 的一个子空间, 且关于 p 次幂封闭. 证明 $\mathfrak{J}$ 关于换位运算也是封闭的, 故 $\mathfrak{J}$ 满足定理 19 的所有条件.

5. 证明: 若 D 是 P 的导子, $\eta \in P$, 则

$$\eta_R D^i = \sum_{j=0}^{i} \binom{i}{j} D^j (\eta D^{i-j})_R.$$

6. 设 D 是代数 $\mathfrak{A}$ 的导子, $\mathfrak{A}[t, D]$ 是形式多项式 $\sum_0^m t^i a_i$ $(a_i \in \mathfrak{A})$ 的集. 相等、加法及用 Φ 的元相乘的定义与普通多项式的相同,乘法定义为

(34) $$\left(\sum_i t^i a_i\right)\left(\sum_j t^j b_j\right) = \sum_{i,j,k} \binom{j}{k} t^{j+k} (a_i D^{j-k}) b_j.$$

验证结合律成立,从而证明 $\mathfrak{A}[t, D]$ 是一个代数.

7. 设 D 是特征 $p \neq 0$ 的域 P 的导子, Φ 是 D 常数子域. 假设 $[P:\Phi] = p^m < \infty$. 则由第 3 题得到: 存在 p 多项式 (32) 使 $D^{p^m} + \beta_1 D^{p^{m-1}} + \cdots + \beta_m D = 0 (\beta_i \in \Phi)$. 令 $P[t, D]$ 是第 6 题所定义的微分多项式的代数. 验证: 若 γ 是 Φ 的任意元, 则

$$\pi(\gamma) \equiv t^{p^m} + t^{p^{m-1}}\beta_1 + \cdots + t\beta_m - \gamma$$

在 $P[t, D]$ 的中心里．$(\pi(\gamma))$ 表示由 $\pi(\gamma)$ 生成的理想．证明，若 $\mathfrak{A}_\gamma = P[t, D]/(\pi(\gamma))$，则 $[\mathfrak{A}_\gamma:\Phi] = p^{2m}$．再证明 $\mathfrak{A}_0 \cong \mathfrak{L}_\Phi(P)$．

8．记号如第 7 题．令 ρ 是 P 的任意元．证明：存在 $P[t, D]$ 的自同构使

$$t \to t + \rho, \quad \eta \to \eta$$

(对一切 $\eta \in P$)．注意由 (34) 得到 $[\rho, t] = \rho t - t\rho = \rho D$，并由此式与 (31) 得到 $(t+\rho)^p = t^p + (\rho^p + \rho D^{p-1})$．更一般地，证明

$$(t+\rho)^{p^j} = t^{p^j} + \rho^{[p^j]}, \tag{35}$$

这里

$$\rho^{[p^j]} = \rho^{p^j} + (\rho D^{p-1})^{p^{j-1}} + (\rho D^{p^2-1})^{p^{j-2}} + \cdots + \rho D^{p^j-1}. \tag{36}$$

9．续第 7 题和第 8 题．证明 $P[t, D]$ 的使 $t \to t + \rho$，$\eta \to \eta\ (\eta \in P)$ 的自同构把 $\pi(\gamma)$ 生成的理想映到其自身当且仅当 ρ 满足

$$\rho^{[p^m]} + \beta_1 \rho^{[p^{m-1}]} + \beta_2 \rho^{[p^{m-2}]} + \cdots + \beta_m \rho = 0. \tag{37}$$

10．续第 7 题至第 9 题．证明：存在 $\mathfrak{L}_\Phi(P)$ 的自同构映每一 $\eta \in P$ 为其自身以及映 $D \to D + 1\rho\ (\rho \in P)$ 当且仅当 ρ 满足 (37)．由此证明希尔伯特定理 90 的以下类比：元 ρ 满足 (37) 当且仅当它是 P 中某个 σ 的"对数导子" $(\sigma D)\sigma^{-1}$．

11．证明以下类似于伽罗瓦情形中第一个上同调群 $H^1(G, P^*) = 0$ 的结果（参考 § 1.15）．设 P 是 Φ 上指数为 1 的纯不可分扩张，$[P:\Phi] = p^m < \infty$．$\mathfrak{D}$ 是 P 在 Φ 上的导子的限制 P 李代数．令 $D \to \mu(D)$ 是 $\mathfrak{D}$ 到 P 内的 P 线性映射（即是 $\mathfrak{D}$ 的共轭空间 $\mathfrak{D}^*$ 的一个元），使

$$\mu(D^p) = \mu(D)^p + \mu(D)D^{p-1}, \tag{38}$$

则存在 $\sigma \in P$ 使 $\mu(D) = (\sigma D)\sigma^{-1}$ 对一切 D 成立．

12．证明，若 $\mathfrak{A}_\gamma$ 如第 7 题所给．如果（和 (37) 一样）对某个 $\rho \in P$

$$\delta - \gamma = \rho^{[p^m]} + \beta_1 \rho^{[p^{m-1}]} + \beta_2 \rho^{[p^{m-2}]} + \cdots + \beta_m \rho, \tag{39}$$

则 $\mathfrak{A}_\gamma \cong \mathfrak{A}_\delta$．利用第 7 题证明：如果存在 $\rho \in P$ 使

$$\gamma = \rho^{[p^m]} + \beta_1 \rho^{[p^{m-1}]} + \cdots + \beta_m \rho$$

（这个条件也是必要的），则 $\mathfrak{A} \cong \Phi_{p^m}$．

13．应用第 1 题证明以下整系数多项式的结果：令 $g(x)$ 是任意这种多项式，定义 $g_k(x) = g_{k-1}(x)g'(x)$，$g_1(x) = g(x)$．其中 $'$ 是标准导数 (standard derivative)．证明：对任何素数 p，$g'_{p-1}(x) \equiv \eta(x^p) \pmod{p}$，此处 $\eta(x)$ 是一个整系数多项式．

14．设 γ 和 δ 是特征 $p \neq 0$ 的 Φ 的元，但不是 Φ 中元素的 p 次幂．利用第 12 题（必要性与充分性）证明

$$(x_0^p + x_{p-1}) + x_1^p \gamma + x_2^p \gamma^2 + \cdots + x_{p-1}^p \gamma^{p-1} = \delta \tag{40}$$

有解 $x_i \in \Phi$ 当且仅当

$$(y_0^p + y_{p-1}) + y_1^p \delta + y_2^p \delta^2 + \cdots + y_{p-1}^p \delta^{p-1} = \gamma \tag{41}$$

有解 $y_i \in \Phi$．

15．D 是特征为 p 的域 P 的非零导子．证明：算子 $1, D, \cdots, D^{p-1}$ 在 P 上右线性无关，如果 $\rho_i \in P$，则 $\rho_0 + D\rho_1 + \cdots + D^{p-1}\rho_{p-1}$ 是一个导子仅当每一 $\rho_i = 0$ $(i \neq 1)$．并证明：若 $\rho \in P$，则

$$(D_\rho)^p = D^p\rho^p + D(\rho E)^{p-1} + \sum_{i}^{p-1} D^i\rho_i,$$

这里 $\rho_i \in P$ 且 $E = D_\rho (= D\rho_K)$. 用这些结果证明以下霍赫希尔德 (Hochschild) 公式:

$$E^p = (D\rho)^p = D^p\rho^p + D(\rho E^{p-1}).$$

16. 研究无限维的指数为 1 的纯不可分扩张的克鲁尔 (Krull) 类型伽罗瓦理论的可能性.

9. 高阶导子 导子可以按下面方法推广.

定义 5. 设 $\mathfrak{A}$ 是 Φ 上代数 $\mathfrak{B}$ 的子代数. 则 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的映射序列 $D^{(m)} = \{D_0 = 1, D_1, \cdots, D_m\}$ 叫作 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的秩 m 高阶导子,假若每个 D_i 是线性的,而且

$$(ab)D_j = \sum_{i=0}^{j} (aD_i)(bD_{j-i}), \quad j = 0, 1, \cdots, m, \tag{42}$$

对每个 $a, b \in \mathfrak{A}$ 成立. 无限秩的高阶导子是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的线性映射的无限序列 $\{D_0 = 1, D_1, \cdots\}$, 且对一切 $j = 0, 1, 2, \cdots$ 使 (42) 式成立.

显然,如果 $\{D_0, D_1, D_2, \cdots\}$ 是无限秩的高阶导子, 则截段 (section) $\{D_0, D_1, \cdots, D_m\}$ 是一个秩 m 的高阶导子. 而且高阶导子 $\{D_0, \cdots, D_m\}$ 的任一截段 $\{D_0, D_1, \cdots, D_q\}$ $(q \leqslant m)$ 也是一个高阶导子. 映射 D_1 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的导子.

令 $\mathfrak{A} = \mathfrak{B} = \Phi[x]$, 这里 x 是超越元,设 D_i 是 $\mathfrak{A}$ 内的线性映射,它在基 $(1, x, x^2, \cdots)$ 上的作用由

$$x^m D_i = \binom{m}{i} x^{m-i} \tag{43}$$

给定, 这里当 $i > m$ 时规定 $\binom{m}{i} = 0$, 则

$$x^{m+n} D_j = \binom{m+n}{j} x^{m+n-j}$$

且

$$(x^m D_i)(x^n D_{j-i}) = \binom{m}{i}\binom{n}{j-i} x^{m+n-j}$$

因为 $\sum_{i=0}^{j}\binom{m}{i}\binom{n}{j-i}=\binom{m+n}{j}$，我们有

$$\sum_{i=0}^{j}(x^m D_i)(x^n D_{j-i})=x^{m+n}D_j.$$

这就表明 $(1, D_1, D_2, \cdots)$ 是 $\Phi[x]$ 中无限秩的高阶导子.

如果Φ的特征为 0，则(43) 表明 $i!D_i=D_1^i$，这里 D_1 是 $\Phi[x]$ 中通常的标准导子，于是 $D_i=\frac{1}{i!}D_1^i$. 更一般地，若 D_1 是特征为 0 的任意代数的导子，定义 $D_i=\frac{1}{i!}D_1^i$，则 $\{1, D_1, D_2, \cdots\}$ 是 $\mathfrak{A}$ 的无限秩的高阶导子，由莱布尼茨公式直接得到:

$$(ab)D^j=\sum_{i=0}^{j}\binom{j}{i}(aD^i)(bD^{j-i}),$$

于是给出 $(ab)(D^j/j!)=\sum(aD^i/i!)(bD^{j-i}/(j-i)!)$. 这就是 (42) 在 $D_i=\frac{1}{i!}D_1^i$ 的情形.

把导子化为同态来研究的方法可加以推广，并用到高阶导子中去. 令 $\mathfrak{T}^{(m)}$ 是Φ上含基 $(1, t, \cdots, t^m)$ 的代数，其中 $t^{m+1}=0$，则 $\mathfrak{T}^{(m)}\cong\Phi[x]/(x^{m+1})$. 令 $\mathfrak{B}^{(m)}=\mathfrak{B}\otimes_\Phi\mathfrak{T}^{(m)}$. 如果 $D^{(m)}=\{1, D_1, \cdots, D_m\}$ 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 的秩m高阶导子. 那末引入 $\mathfrak{A}$ 到 $\mathfrak{B}^{(m)}$ 的映射 $(D^{(m)})$

(44) $\quad a\to a+(aD_1)t+(aD_2)t^2+\cdots+(aD_m)t^m$

显然 $s=s(D^{(m)})$ 是线性的. 此外还有

$$\begin{aligned}a^s b^s&=\sum_0^m(aD_i)t^i\sum_0^m(bD_k)t^k\\&=\sum_0^m\sum_{i=0}^{j}(aD_i)(bD_{j-i})t^j\\&=\sum_0^m(ab)D_jt^j\\&=(ab)^s.\end{aligned}$$

这就表明 s 是 $\mathfrak{A}$ 到 $\mathfrak{B}^{(m)}$ 内的一个同态。我们有同态

$$\pi: a_0 + a_1 t + a_2 t^2 + \cdots + a_m t^m \to a_0 \quad (a_i \in \mathfrak{B}),$$

使每一 $a \in \mathfrak{A}$ 满足 $a^{s\pi} = a$. 和导子的特殊情形一样，这个性质刻划了从秩 m 高阶导子可得到同态 s.

将类似的想法运用到无限秩高阶导子中来，我们可用幂级数

$$(45) \qquad a_0 + a_1 t + a_2 t^2 + \cdots \quad (a_i \in \mathfrak{B})$$

的代数 $\mathfrak{B}[[t]]$ (参考卷 1 的中译本 p. 89) 代替代数 $\mathfrak{B}^{(m)}$. 如前所述，若 $\{1, D_1, \cdots\}$ 是无限秩的高阶导子，则映射

$$s: a \to a + (aD_1)t + (aD_2)t^2 + \cdots$$

是 $\mathfrak{A}$ 到 $\mathfrak{B}[[t]]$ 内的同态，它满足 $a^{s\pi} = a$ (对一切 $a \in \mathfrak{A}$)，这里 π 是同态 $\sum a_i t^i \to a_0$. 相反地，如果 $a \to a^s$ 是 $\mathfrak{A}$ 到 $\mathfrak{B}[[t]]$ 内满足 $a^{s\pi} = a$ $(a \in \mathfrak{A})$ 的同态，则可写成

$$a^s = a + (aD_1)t + (aD_2)t^2 + \cdots,$$

而且 $\{D_0 = 1, D_1, D_2, \cdots\}$ 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的高阶导子。

设 $\{D_i\}$ 是 $\mathfrak{A}$ 到 $\mathfrak{B}$ 内的秩 m (或无限秩) 的高阶导子，称元 $a \in \mathfrak{A}$ 关于高阶导子是**常数**，假若对一切 $i > 0$ 有 $aD_i = 0$. 这即是说在与高阶导子相关的同态 s 之下，有 $a^s = a$. 因此常数集显然是代数 $\mathfrak{A}$ 的子代数.

本节目的是引入高阶导子并对纯不可分域的高阶导子作简短的研究. 设 P/Φ 是一个特征 $p \neq 0$ 的域，E 是 P/Φ 的子域，

$$D^{(m)} = \{1, D_1, D_2, \cdots, D_m\}$$

是 E/Φ 内的秩 m 高阶导子. 一般来说，若

$$D_1 = D_2 = \cdots = D_{q-1} = 0$$

而 $D_q \neq 0$，我们就把这个高阶导子称为是 q **阶**的. 假若 $D_1 \neq 0$ 则称 $D^{(m)}$ 是**真**高阶导子. 若阶为 q，则 E 到 $\mathrm{P}^{(m)}$ 内的相伴同态 (*associated homorphism*) $s = s(D^{(m)})$ 有形式：

$$(46) \qquad \varepsilon \to \varepsilon + (\varepsilon D_q)t^q + (\varepsilon D_{q+1})t^{q+1} + \cdots + (\varepsilon D_m)t^m,$$

其中，对 E 的某个元 $\varepsilon \in D_q \neq 0$. 由此证明以下

定理 20. 设 P/Φ 是特征 $p \neq 0$ 的域，E 是 P/Φ 的子域，$D^{(m)}$ 是 E/Φ 到 P/Φ 内的秩 m、q 阶高阶导子. Γ 是 E 的 $D^{(m)}$

常数子域，p^e 是大于 $\frac{m}{q}$ 的 p 的最小次幂，那末 E 是 Γ 上指数为 e 的纯不可分扩张

证　我们必须证明 $\varepsilon^{p^e}\in\Gamma$（对每一 $\varepsilon\in E$）和存在 $\varepsilon\in E$ 使 $\varepsilon^{p^{e-1}}\notin\Gamma$。前者是显然的，因为由 (46)

$$(\varepsilon^{p^e})^s=(\varepsilon^s)^{p^e}=(\varepsilon+(\varepsilon D_q)t^q+\cdots)^{p^e}$$
$$=\varepsilon^{p^e}+(\varepsilon D_q)^{p^e}t^{p^eq}+\cdots=\varepsilon^{p^e}.$$

所以 $\varepsilon^{p^e}\in\Gamma$。现在选取 ε 使 $\varepsilon D_q\neq 0$，则

$$(\varepsilon^{p^{e-1}})^s=\varepsilon^{p^{e-1}}+(\varepsilon D_q)^{p^{e-1}}t^{p^{e-1}q}+\cdots.$$

因为 $p^{e-1}q\leqslant m$，显然 $(\varepsilon^{p^{e-1}})^s\neq\varepsilon^{p^{e-1}}$。所以 $\varepsilon^{p^{e-1}}\notin\Gamma$。

其次，我们考虑纯不可分单扩张域 $\mathrm{P}=\Phi(\xi)$，这里 $x^{p^e}-\alpha$ 是 ξ 在 Φ 上的最小多项式。令 $\{D_i\}$ 是由 (43) 定义的多项式代数 $\Phi[x]$ 的高阶导子。令 $D^{(p^e-1)}=\{1,D_1,\cdots,D_{p^e-1}\}$ 是秩 p^e-1 的高阶导子，它是这个高阶导子 $\{D_i\}$ 的一个截段，我们有

$$(x^{p^e}-\alpha)D_j=0\ (1\leqslant j\leqslant p^e-1).$$

它及关系 (42) 推出主理想 $\mathfrak{I}=(x^{p^e}-\alpha)$ 在每个 D_j 下映入其自身，所以每个 D_j 导出一个 $\mathrm{P}=\Phi(\xi)\cong\Phi[x]/\mathfrak{I}$ 内的线性映射，我们还是将它记作 D_j。D_i 在 $\Phi[x]$ 中的条件 (42) 转化为 D_i 在 $\Phi(\xi)$ 中的同样条件。因此得到在 $\Phi(\xi)$ 中使

$$\xi^mD_i=\binom{m}{i}\xi^{m-i},\ m=0,1,\cdots,p^e-1 \tag{47}$$

的高阶导子 $D^{(p^e-1)}$。现在来证明 $D^{(p^e-1)}$ 的 $\{D_i\}$ 常数子域 Γ 就是 Φ。假设 $\Phi\subset\Gamma$，则 ξ 在 Γ 上的最小多项式是 $x^{p^f}-\beta$（$f<e$，$\beta\in\Gamma$），因此 $\xi^{p^f}\in\Gamma$。另一方面，定义 (47) 给出 $\xi^{p^f}D_{p^f}=1$，这就证明了我们的论断。

次设 P 是 Φ 的纯不可分扩张，而且 P 是单扩张 $\mathrm{P}_1,\mathrm{P}_2,\cdots,\mathrm{P}_r$，$\mathrm{P}_i=\Phi(\xi_i)$ 的一个张量积。这就是说 $\mathrm{P}=\Phi(\xi_1,\xi_2,\cdots,\xi_r)$，而且单项式 $\xi_1^{k_1}\xi_2^{k_2}\cdots\xi_r^{k_r}$，$(0\leqslant k_i<p^{e_i})$ 构成 P 在 Φ 上的一个基。如果设 $\Phi_i=\Phi(\xi_1,\cdots,\xi_{i-1},\xi_{i+1},\cdots,\xi_r)$，则 $\mathrm{P}=\Phi_i(\xi_i)$，

$$\Phi_1\cap\Phi_2\cap\cdots\cap\Phi_r=\Phi.$$

在P中存在高阶导子，其常数是Φ_i的元．从而Φ是P中关于P在Φ上的一切有限秩高阶导子为常数的所有元组成的子集．

习　　题　　34

1．设$\{D_i\}$是由(43)定义的$\Phi[x]$的高阶导子，x是超越元．证明

$$f(x+\alpha)=f(\alpha)+(fD_1)(\alpha)x+(fD_2)(\alpha)x^2+\cdots.$$

2．令$\Phi[x_1,x_2,\cdots,x_m]$是域Φ上未定元x_i的多项式代数．$(k_1,k_2,\cdots,k_m)$是非负整数序列．我们在$\Phi[x_1,x_2,\cdots,x_m]$中定义一个线性算子$D_{k_1k_2\cdots k_m}$，它在基元$(x_1^{n_1}x_2^{n_2}\cdots x_m^{n_m})$上的作用如下：

$$(x_1^{n_1}x_2^{n_2}\cdots x_m^{n_m})D_{k_1k_2\cdots k_m}=\begin{cases}0, & \text{若任何 } k_i>n_i\\ \binom{n_1}{k_1}\binom{n_2}{k_2}\cdots\binom{n_m}{k_m}x_1^{n_1-k_1}x_2^{n_2-k_2}\cdots x_m^{n_m-k_m}, & \text{若 } k_i\leqslant n_i.\end{cases}$$

证明：如果$f(x_1,x_2,\cdots,x_m)\in\Phi[x_1,x_2,\cdots,x_m]$而且$\alpha_1,\alpha_2,\cdots,\alpha_m\in\Phi$，则

$$f(x_1+\alpha_1,x_2+\alpha_2,\cdots,x_m+\alpha_m)=\sum_{k_i}(fD_{k_1k_2\cdots k_m})_{x_j=\alpha_j}x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}.$$

3．设$f(x_1,\cdots,x_m)$是$\Phi[x_1,x_2,\cdots,x_m]$中次数$n\leqslant m$的一个齐次多项式．若存在一个$\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_m)$，$(\alpha_i\in\Phi)$，使得当$\Sigma k_i\leqslant n-2$时有

$$(fD_{k_1k_2\cdots k_m})_{x_j=\alpha_j}=0$$

成立，而且

$$\sum_{k_1+k_2+\cdots+k_m=n-1}(fD_{k_1k_2\cdots k_m})_{x_j=\alpha_j}x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}\neq 0.$$

证明方程$f(x_1,x_2,\cdots,x_m)=\beta$对任何$\beta\in\Phi$在$\Phi$中有一个解．由此证明

$$x^3+y^3+z^3-3xyz=\beta$$

在任何特征$\neq 3$的域中可解．

4．$\mathfrak{A}$的无限秩高阶导子称为**迭代的**，假若

$$D_iD_j=\binom{i+j}{i}D_{i+j},$$

高阶导子$D^{(m)}=\{D_i\}$叫作**迭代的**，假若当$i+j\leqslant m$时有$D_iD_j=\binom{i+j}{i}D_{i+j}$，而当$i+j>m$时有$D_iD_j=0$．验证由(43)与(47)定义的高阶导子是迭代的．

5．令$P=\Phi(\xi)$，Φ的特征$p\neq 0$，ξ在Φ上的最小多项式是$x^{p^e}-\alpha$．证明P/Φ的子域是域$\Phi(\xi^{p^f})$，这里$0\leqslant f\leqslant e$．并证明这$e+1$个子域是互不相同的．

6．韦斯菲尔德(Weisfeld)设Φ_0是特征$p\neq 0$的域，$\Phi=\Phi_0(\alpha,\beta,\gamma)$，这里$\alpha^p,\beta^p,\gamma^p\in\Phi_0$，这些元素在$\Phi_0$上是$p$无关的($[\Phi:\Phi_0]=p^3$)．令$P=\Phi(\xi,\eta)$其中$\xi^{p^2}=\alpha$，$\eta^p=\beta\xi^p+\gamma$．证明$[P:\Phi]=p^3$．证明$[\Phi(\xi):\Phi]=p^2$，

$$[\Phi(\eta):\Phi]=p^2,$$

而且 $\Phi(\xi)\cap\Phi(\eta)=\Phi$. 并证明: $P\neq\Phi(\xi,\zeta)$, $P\neq\Phi(\eta,\zeta)$, 这里ζ是使 $\zeta^p\in\Phi$ 的任何元. 由此证明 P/Φ 不是单扩张的张量积.

7. 证明$\{D_i\}$是高阶导子当且仅当 $a_R D_j=\sum_{i=0}^{j} D_i(aD_{j-i})_R$, $j=0,1,\cdots$. 证明: 若高阶导子 $\{1,D_1,D_2,\cdots,D_m\}$ 中, $D_1\neq 0$, 则 $(P,+)$ 的自同态$(1,D_1,\cdots,D_m)$ 是右P无关的.

8. 令 $D_{(p^e-1)}$ 是特征为p的域D中的秩 p^e-1 迭代高阶导子. 假设 $D^{(p^e-1)}$ 是真高阶导子,Φ是常数子域. 证明: P在Φ上的每一线性变换形如

$$\sum_{0}^{p^e-1} D_i\rho_i\equiv\Sigma D_i\rho_i R\ (\rho_i\in P).$$

而且 $P=\Phi(\xi)$, 这里ξ在Φ上的最小多项式是 $x^{p^e}-\alpha$.

9. 续第8题证明 P/Φ 中线性变换序列 $\{d_0,d_1,\cdots,d_{p^e-1}\}$ 满足

$$\rho_R d_j=\sum_{i=0}^{j} d_i(\rho D_{j-i}),\ j=0,1,\cdots,p^e-1,$$

当且仅当存在向量 $(\sigma_0,\sigma_1,\cdots,\sigma_{p^e-1})$, $\sigma_0=1$, $\sigma_i\in P$. 使

$$d_i=D_i\sigma_0+D_{i-1}\sigma_1+\cdots+1\sigma_i.$$

利用上述结论给出向量 $(\sigma_0,\sigma_1,\cdots,\sigma_{p^e-1})$ 为"对数导数"的充要条件.$(\sigma_0,\sigma_1,\cdots,\sigma_{p^e-1})$为"对数导数"的意义是: 存在$\rho\in P$使得 $\sigma_i=\rho^{-1}(\rho D_i)$, $i=0,1,\cdots,p^e-1$).

10. 域的张量积 在第一章中, 我们考虑过两个域的张量积, 其中一个在基域上是有限维的. 我们看到,要了解域 P/Φ 和 E/Φ 的合成 ($[P:\Phi]<\infty$), 有必要弄清 $P\otimes_\Phi E$ 的极大理想.本节与下节将这些结果推广到任意域上. 首先要将其中有一域是代数扩张时的若干结果汇总起来. 我们所说的可分性是在 (本章的第五节末)一般意义下定义的. 纯不可分性是指纯不可分代数扩张.还要说明, 子域Φ在P中是代数封闭的(可分代数封闭), 假若 P/Φ 的每个代数元(可分代数元)含于Φ中. 现给出以下

定理21. 设 P/Φ 和 E/Φ 是Φ的扩域.

(1) 若 P/Φ 是可分的而 E/Φ 是纯不可分的. 则 $P\otimes_\Phi E$ 是域. 另一方面,若 P/Φ 不是可分的,则存在指数为1的纯不可分扩张 E/Φ, 使 $P\otimes_\Phi E$ 包含一个非零幂零元.

(2) 若 P/Φ 是可分代数的,则对任何 E/Φ, $P\otimes_\Phi E$ 没有非零幂零元. 若Φ在E中是可分代数封闭的,则 $P\otimes_\Phi E$ 是一个域.

(3) 假若 P/Φ 是纯不可分的,而 E/Φ 是任意的,或者 P/Φ

是代数的而Φ在E中是可分代数封闭的．则 $\mathrm{P}\otimes_{\Phi}E$ 的元是单位或是幂零的．

证　在(1)中及在(3)的第一部分中可设特征 $p\neq 0$．在所有情形下，我们都将 $\mathrm{P}\otimes_{\Phi}E$ 写成 $\mathrm{P}\otimes E$，并将P和E看作

$$\mathrm{P}\otimes E=\mathrm{P}E$$

的子代数．它们是线性不相交的．因此满足已讲过的各种线性无关性质．

(1) 设 P/Φ 可分而E/Φ纯不可分．由可分性推出：若 $\rho_1,\rho_2,\cdots,\rho_m$ 是P的Φ无关元，则对每个 $e=0,1,2,\cdots$，元 $\rho_1^{p^e},\rho_2^{p^e},\cdots,\rho_m^{p^e}$ 是Φ无关的．令设

$$z=\sum_1^m \rho_i\sigma_i\in\mathrm{P}\otimes E,$$

这里 $\rho_i\in\mathrm{P}$，$\sigma_i\in E$．我们可以假设ρ_i是Φ无关的．若$z\neq 0$，则还可设每个 $\sigma_i\neq 0$． 因为 E/Φ 是纯不可分的，故存在正整数e使 $\sigma_i^{p^e}=\alpha_i\in\Phi$ $(1\leqslant i\leqslant m)$，则 $z^{p^e}=\sum\alpha_i\rho_i^{p^e}\in\mathrm{P}$．若$z\neq 0$，则$\alpha_i\neq 0$ 且 z^{p^e} 是P的非零元．因此z^{p^e}有逆元，从而z也有逆元．于是$\mathrm{P}\otimes E$是域． 下面设 P/Φ 不是可分的，则P中存在元 $\rho_1,\rho_2,\cdots,\rho_m$ 是Φ无关的．但Φ中有 $\gamma_i\neq 0$ 使 $\Sigma\gamma_i\rho_i^p=0$．并非所有γ_i都是Φ中元的p次幂．所以 $E=\Phi(\sigma_1,\sigma_2,\cdots,\sigma_m)$（其中 $\sigma_i^p=\gamma_i$）是Φ上指数为1的扩张域．因为ρ_i是Φ无关的，且$\sigma_i\in E$，故$\mathrm{P}\otimes E$的元 $z=\Sigma\rho_i\sigma_i$ 不为0．另一方面，

$$z^p=\Sigma\rho_i^p\sigma_i^p=\Sigma\gamma_i\rho_i^p=0.$$

(2) 设 P/Φ 是可分代数的，E/Φ 是任意的，需要证明$\mathrm{P}\otimes E$没有非零幂零元，而且当Φ在E中是可分代数封闭时，$\mathrm{P}\otimes E$是一个域．设 $z\in\mathrm{P}\otimes E$，$z=\sum_1^m\rho_i\sigma_i$，$\rho_i\in\mathrm{P}$，$\sigma_i\in E$．因为 P/Φ 是代数的，故这些ρ_i生成一个有限维扩张．在证明过程中显然可用这个扩张代替P．因此可以假设 $[\mathrm{P}:\Phi]<\infty$． 由P的可分性推出 $\mathrm{P}=\Phi(\theta)\cong\Phi[x]/(f(x))$，$f(x)$ 在 $\Phi[x]$ 中是可分的而且是不可约的．由第一章可见(中译本 p.86)，

$$\mathrm{P}\otimes E\cong E[x]/(f(x)).$$

所以只要证明 $E[x]/(f(x))$ 没有非零幂零元，而且当Φ在E上是可分代数封闭时它是一个域就行了．在第一章曾经看到，$E[x]/(f(x))$是域的直和，而且容易验证：具有这种构造的代数不包含非零幂零元．这就证明了第一个论断．下面设 $E[x]/(f(x))$不是域，则在 $E[x]$ 中 $f(x)=g(x)h(x),\deg g(x)>0,\deg h(x)>0$．设$\Omega$是 $f(x)$在Φ上的分裂域，且在 $\Omega[x]$ 中 $f(x)=\Pi(x-\omega_i)$．因为ω_i是 $f(x)$ 的根，它们是Φ上的可分代数元，于是 $g(x)$ 和 $h(x)$ 的系数也是Φ上的可分代数元，因为 $f(x)$ 在 $\Phi[x]$ 上不可约，所以这些系数是E的元而且不全含于Φ．因此Φ在E中不是可分代数封闭的．

(3) 首先假设 P/Φ 是纯不可分的，E/Φ 是任意的．令

$$z=\sum_{1}^{m}\rho_i\sigma_i\in\mathrm{P}\otimes E,$$

$\rho_i\in\mathrm{P}$，$\sigma_i\in E$．选择 $e>0$ 使 $\rho_i^{p^e}=\alpha_i\varepsilon\Phi$，则 $z^{p^e}=\Sigma\alpha_i\sigma_i^{p^e}\varepsilon E$，则或者 $z^{p^e}=0$ 或者 z^{p^e} 在E中有逆元．在后一情形下，z是 $\mathrm{P}\otimes E$ 的单位．下面设P/Φ是代数的，Φ在E中是可分代数封闭的．令Σ/Φ 是 P/Φ 的最大可分子域，则 $\mathrm{P}E=\mathrm{P}\otimes E$ 在Φ上的子代数 ΣE 是 Σ/Φ 与 E/Φ 的张量积．因为Φ在E中是可分代数封闭的，由(2)得 $\Sigma E=\Sigma\otimes E$ 是一个域．令$\{\rho_\alpha\}$是P/Σ的一个基，$\{\sigma_\beta\}$是Σ/Φ的一个基，则 $\{\rho_\alpha\sigma_\beta\}$ 是 P/Φ 的一个基而且这些元在 $\mathrm{P}\otimes E$ 中是E无关的，于是元ρ_α是ΣE无关的．这就推出：如果把P与ΣE看作Σ上的代数，则 $\mathrm{P}(\Sigma E)=\mathrm{P}\otimes_\Sigma\Sigma E$．另一方面，$\mathrm{P}(\Sigma E)$ 与 $\mathrm{P}E=P\otimes_\Phi E$ 是Φ上的同一的代数．因此只要证明 $\mathrm{P}\otimes_\Sigma\Sigma E$ 的每一元是幂零元或是单位就够了．因为 P/Σ 是纯不可分的，由现在所证的第一部分就可得证[1]．

我们的下一个目标是要得到两个域(其一是纯超越的)的张量

1) 证明中用到 $\mathrm{P}\otimes_\Phi E$ 和 $\mathrm{P}\otimes_\Phi(\Sigma\otimes_\Phi E)$ 是相同的．这可由张量积的一般公式得到．由结合性：$\mathrm{P}\otimes_\Sigma(\Sigma\otimes_\Phi E)\cong(\mathrm{P}\otimes_\Sigma\Sigma)\otimes_\Phi\Phi$（参考本书导言第三节习题中的第5题）．此外，$\mathrm{P}\otimes_\Sigma\Sigma\cong\mathrm{P}$，故 $\mathrm{P}\otimes_\Sigma(\Sigma\otimes_\Phi E)\cong\mathrm{P}\otimes_\Phi E$．——著者注．

积的一些结果，我们要证明以下

定理 22. 设 P 是 Φ 上的纯超越扩张即 $\mathrm{P}=\Phi(B)$，这里 B 是一个超越基．E/Φ 是任意的．则 $\mathrm{P}\otimes_\Phi E$ 没有零因子．设 Ω 是它的分式域，则 $\Omega=E(B)$ 是 E 上以 B 为超越基的纯超越扩张．此外，若 Φ 在 E 中是代数封闭的（可分代数封闭的），则 $\mathrm{P}=\Phi(B)$ 在 $\Omega=E(B)$ 中是代数封闭的（可分代数封闭的）．

证　我们照例把 P 和 E 看作 $\mathrm{P}\otimes_\Phi E$ 的子代数，因为 B 是代数无关集，不同的单项式 $\beta_1^{k_1}\beta_2^{k_2}\cdots\beta_r^{k_r}$ $(k_i\geq 0,\beta\in B)$ 的集 M 形成由 B 生成的子代数 $\Phi[B]$ 的一个基．因为 $\Phi[B]$ 与 E 是线性不相交的，所以 M 是 E 无关的．故 B 在 $E[B]$ 中是代数无关的．由此可见，若 F 是 B 的有限子集，则 $E[F]$ 没有零因子（卷 1 的中译本 p. 99）．因此 $E[B]$ 是一个整区，故它有商域 Ω，其元有形式 $\mathrm{P}Q^{-1}$，这里 $\mathrm{P},Q\in E[B]$．可见 $\Omega=E(B)$．而 B 是 E 上的代数无关集，故 Ω 是 E 上的以 B 为超越基的纯超越扩张．再来考察 Ω 所含的形为 $\mathrm{P}q^{-1}$ 的元的子代数 Ω_1，这里 $\mathrm{P}\in E[B]$，

$$q\in\Phi[B].$$

我们来证明这个子代数恒同于 $\mathrm{P}\otimes_\Phi E$．首先，我们有 $E[B]\subseteq\Omega$ 到 $E[B]\subseteq\mathrm{P}\otimes_\Phi E$ 内的恒等同构．由导言的 I，这个同构可唯一地扩张为 $\Omega_1=\{\mathrm{P}q^{-1}|\mathrm{P}\in E[B],0\neq q\in\Phi[B]\}$ 到 $\mathrm{P}\otimes_\Phi E$ 内的同构．这是因为 $\mathrm{P}=\Phi(B)$ 中存在 q^{-1}．设 z 是 $\mathrm{P}\otimes_\Phi E$ 的任意元，它可以写成 $z=\sum\rho_i\varepsilon_i$，$\rho_i\in\mathrm{P}=\Phi(B)$，$\varepsilon_i\in E$．而且

$$\rho_i=p_iq^{-1},\ p_i,\ q\in\Phi[B],$$

故 $z=\sum(p_i\varepsilon_i)q^{-1}=\mathrm{P}q^{-1}$，这里 $\mathrm{P}\in E[B]$．于是 z 是在 Ω_1 的同构象内，故 Ω_1 同构于 $\mathrm{P}\otimes_\Phi E$．我们若将 $\mathrm{P}\otimes_\Phi E$ 与 Ω_1 等同起来，由于 $\Omega_1\supseteq\Phi[B]$，可见 Ω 也是 Ω_1 的分式域．这就证明了第一个论断．为了证明第二个论断我们要证明：若 $\Omega=E(B)$ 包含不属于 $\Phi(B)$ 的 $\Phi(B)$ 上的代数元（可分代数元），则 E 包含不属于 Φ 的 Φ 上的代数元（可分代数元）．显然，如果 $\Omega=E(B)$ 中存在这种类型的元，则它也属于 $E(F)$，这里 F 是 B 的有限子集．因此可以取 B 是有限的．由归纳法可知，只要证明以下结果：令

E/Φ 是任意域，ξ 是 E 上的超越元．如果 $E(\xi)$ 包含一个不属于 $\Phi(\xi)$ 的 $\Phi(\xi)$ 上的代数元(可分代数元)，则 E 含有一个不属于 Φ 的 Φ 上的代数元(可分代数元)．为此，令 η 是 $E(\xi)$ 的一个元，它是 $\Phi(\xi)$ 上的代数元．令 $x^n+\beta_1x^{n-1}+\cdots+\beta_n$ 是 η 在 $\Phi(\xi)$ 上的最小多项式．系数可写成 $\beta_i=p_iq^{-i}$[1]，这里 $p_i, q\in\Phi[\xi]$ (例如，q 可取作 β_i 的分母的乘积)，则 $H=q\eta$ 是 $\Phi(\xi)$ 上最小多项式为 $x^n+p_1x^{n-1}+p_2x^{n-2}+\cdots+p_n$ 的代数元．如果 $H=PQ^{-1}$，其中 $P, Q\in E[\xi]$，且是互素的多项式，则 H 的方程给出

$$P^n=-p_1P^{n-1}Q-p_2P^{n-2}Q^2-\cdots-p_nQ^n.$$

如果 Q 是正次数的，则 Q 有一个不可约因子，而上述关系表明它是 P^n 的因子．从而也是 P 的因子，这与 P, Q 的假设矛盾．所以 Q 是单位，而且 $H\in E[\xi]$．设 $H=\varepsilon_0+\varepsilon_1\xi+\varepsilon_2\xi^2+\cdots+\varepsilon_m\xi^m$，$\varepsilon_i\in E$．我们要证明：由关系 $O=H(\xi)^n+p_1(\xi)H(\xi)^{n-1}+\cdots+p_n(\xi)$，$H=H(\xi)$，$p_i=p_i(\xi)\in\Phi[\xi]$ 推出系数 ε_i 是 Φ 上的代数元．设 $\alpha\in\Phi$，考虑 $E[\xi]$ 到 E 内的 E 同态：$\xi\to\alpha$．因为 ξ 是超越元，所以这样的同态存在．照例将 $Q(\xi)$ 的象记作 $Q(\alpha)$，则有关系式 $H(\alpha)^n+p_1(\alpha)H(\alpha)^{n-1}+\cdots+p_n(\alpha)=0$．因为 $p_i(\alpha)\in\Phi$，这就表明 $\beta=H(\alpha)$ 是 Φ 上的代数元．先假设 Φ 包含 $m+1$ 个不同元 $\alpha_1, \alpha_2, \cdots, \alpha_{m+1}$，则 $H(\alpha_k)=\sum_{j=0}^{m}\varepsilon_j\alpha_k^j=\beta_k$ 是 Φ 上的代数元 $(k=1,2,\cdots,m+1)$．因为范德蒙德行列式

$$\det(\alpha_k^j)\neq 0,$$

这些关于 ε_j 的方程有唯一解，且可由通常的行列式公式求出，所以 ε 是 Φ 上的代数元．如果 Φ 没有 $m+1$ 个元，这个论证就得按以下方式稍作修改：设 p 是特征，选取 r 使 $p^r>m$． 令 $\bar{E}$ 是 $x^{p^r}-1$ 在 E 上的分裂域，$\bar{\Phi}$ 是 $\bar{E}$ 在 Φ 上的代数元所成子域．显然 $\bar{\Phi}$ 有 $m+1$ 个不同元 α_k．我们就在这些元上进行论证，将 E 用 $\bar{E}$ 代替，Φ 用 $\bar{\Phi}$ 代替．和前面一样我们可以断定 ε_j 是 $\bar{\Phi}$ 上的代数

---

1) 原书误为 q^{-1}．——译者注．

元，因此也是Φ上的代数元．如果所说的$\eta\notin\Phi(\xi)$，则$H\notin\Phi(\xi)$，因而$H=\sum\varepsilon_i\xi^i$中的ε_i不能全在Φ中．因此E中存在不属于Φ[1]的Φ上的代数元．次设$\eta\notin\Phi(\xi)$且η是$\Phi(\xi)$上的可分元，则$H\notin\Phi(\xi)$且是$\Phi(\xi)$上的可分代数元．那末ε_i是代数元而且域$\Phi(\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_m)$含有不属于$\Phi$的可分代数元．否则，因其特征为$p$，就有$\varepsilon_i^{p^e}\in\Phi$（对某个$e=1,2,\cdots$），那末$H^{p^e}\in\Phi(\xi)$．与$H$在$\Phi(\xi)$上的可分性矛盾，证毕．

现在开始处理"混合"类型，即既非代数的也非纯超越的域．首先证明定理 21 的部分结论的推广

定理 23. 设 P/Φ 是可分的，而 E/Φ 是任意的．则 $\mathrm{P}\otimes_\Phi E$ 没有非零幂零元．

证　显然只要在P是有限生成的条件下加以证明即可．此时P是可分生成的，故P有一个超越基B使P在$\Phi(B)$上是可分代数的．考虑由$\Phi(B)$与E生成的子代数$\Phi(B)E=\Phi(B)\otimes_\Phi E$，把它和P一样看作是域$\Phi(B)$上的代数．若$\{\rho_\alpha\}$是P在$\Phi(B)$上的基，则形如$\Sigma c_i\rho_i=0$ $(c_i\in\Phi(B)E)$的关系式仅当每个$c_i=0$时成立．这就推出$\mathrm{P}\otimes_\Phi E=\mathrm{P}\otimes_{\Phi(B)}\Phi(B)E$[2]．把定理 22 应用于$\Phi(B)E=\Phi(B)\otimes_\Phi E$，则$\Phi(B)E$可以嵌入域$\Omega=E(B)$中，而且$\mathrm{P}\otimes_{\Phi(B)}\Phi(B)E$是$\mathrm{P}\otimes_{\Phi(B)}\Omega$的子代数，此处$\Omega$是$\Phi(B)$上的域．因此只要证明$\mathrm{P}\otimes_{\Phi(B)}\Omega$没有非零幂零元即可．又因为P在$\Phi(B)$上是可分代数的，再由定理 21(2) 即得$\mathrm{P}\otimes_{\Phi(B)}\Omega$没有非零幂零元．

以下设P是任意的而Φ在E中是可分代数封闭的．令B是P在Φ上的一个超越基，和前面证明一样，$\mathrm{P}\otimes_\Phi E=\mathrm{P}\otimes_{\Phi(B)}\Phi(B)E$，而且它是$\mathrm{P}\otimes_{\Phi(B)}\Omega$的子代数，其中$\Omega$是域$E(B)$．由定理 22 知道，$\Phi(B)$在$\Omega$中是可分代数封闭的．因为P在$\Phi(B)$上是代数的，定理 21 (3) 表明$\mathrm{P}\otimes_{\Phi(B)}\Omega$的每一元或是幂零元或是单位．今

---

1) 原书误为 E.——译者注.

2) 对此有更精彩的论证，参看 p.194.——著者注.

设 z 是 $\mathrm{P}\otimes_\Phi E\subseteq \mathrm{P}\otimes_{\Phi(B)}\Omega$ 的任意元,则 z 不是幂零元就是 $\mathrm{P}\otimes_{\Phi(B)}\Omega$ 的单位. 在后一情况下, z 不是 $\mathrm{P}\otimes_\Phi E$ 的零因子. 因此我们得到如下:

定理 24. 设 P 是域 Φ 的任意扩张域,Φ 在 E 中是可分代数封闭的. 则 $\mathrm{P}\otimes_\Phi E$ 的每个零因子都是幂零的.

最后两个定理显然有以下直接推论.

推论 1. 设 P 和 E 是 Φ 的两个扩张域且使 (1) P/Φ 或 E/Φ 是可分的, (2) Φ 在 P 或 E 中是可分代数封闭的, 则 $\mathrm{P}\otimes_\Phi E$ 是一个整区.

特别地,如果 P/Φ 是可分的, Φ 在 P 中是代数封闭的, 则对任何 E/Φ, $\mathrm{P}\otimes_\Phi E$ 是一个整区, 满足这两个条件的扩张 P/Φ 叫作*正则的*. 若 Φ 是代数封闭的,则它是完全的,所以任何扩张 P/Φ 是可分的. 因此代数闭域的每一扩张是正则的,因而有

推论 2. 设 Φ 是代数封闭的, 则对 Φ 的任何扩张域 P 和 E, $\mathrm{P}\otimes_\Phi E$ 是一个整区.

11. 域的自由合成 我们记得,Φ 上两个域 E 和 P 的合成是一个三元组 (Γ, s, t), 这里 Γ 是 Φ 上的域, s, t 分别是 Φ 上的 E 和 P 到 Γ 内的同构,而 Γ 是由象 E^s 和 P^t 生成的 (§ 1.16). E 和 P 的合成 (Γ, s, t) 与 (Γ', s', t') 是等价的,假如存在 Γ 到 Γ' 上的同构 u 使 $s'=us$, $t'=ut$. 在 § 1.16 我们已经研究了有限维扩张 P 与另一扩张的合成. 在代数几何中对下面这种域的合成比较感兴趣,这时的域不一定是代数的,对这概念有以下的限制:

定义 6. E/Φ 和 P/Φ 的域合成 (Γ, s, t) 称为自由合成,假若对于 E 和 P 的任何代数无关子集 C 和 D, 集 C^s, D^t 是不相交的,且 $C^s\cup D^t$ 在 Γ/Φ 中是代数无关的.

因为任何代数无关集可以嵌入一个超越基中,显然,(Γ, s, t) 是自由合成这个条件等价于: 对于 E/Φ 和 P/Φ 的每一对超越基 B 和 B', B^s 和 B'^t 是不相交的, 且 $B^s\cup B'^t$ 是代数无关的. 现在考察一下,条件中"每"字可以用"某"字代替. 假设 E/Φ 存在超越基 B, P/Φ 存在超越基 B'. 它们能使 B^s 和 B'^t 是不相交的,

$B^s \cup B''$ 是代数无关的，那末我们就可以断定，这个合成 Γ 是自由合成．显然只要对有限集 C, D 验证定义的条件就行了．在 B 中可以找到有限子集 F 使 C 和 F 在 Φ 上是代数相关的．因为 F 是 B 的子集，F^s 与 D^t 在 Γ 中是代数无关的．因此 $F^s(\subseteq\Phi(F^s, D^t))$ 在 $\Phi(D^t)$ 上是代数无关的．这就推出 $\Phi(F^s, C^s, D^t)$ 在 Φ 上的超越次数是 $f+d$，这里 f 是基数 $|F|$ 而 $d=|D|$（参考 § 3 习题中的第 3 题）．因为 $\Phi(F^s, C^s)$ 在 Φ 上的超越次数是 f，而且 C^s 是代数无关的，$\Phi(F^s, C^s)$ 在 $\Phi(C^s)$ 上的超越次数是 $f-c$，这里 $c=|C|$．于是 $\Phi(F^s, C^s, D^t)$ 在 $\Phi(C^s, D^t)$ 上的超越次数不超过 $f-c$．由此及关于 $\Phi(F^s, C^s, D^t)$ 在 Φ 上的超越次数的公式推出 $\Phi(C^s, D^t)$ 在 Φ 上的超越次数至少是

$$(f+d)-(f-c)=d+c.$$

于是 C^s, D^t 是不相交的，而且 $C^s \cup D^t$ 是代数无关的．将此结果叙述如下：

引理 1. 设 (Γ, s, t) 是 Φ 上的域 E 和 Φ 上的域 P 的域合成．假如 E 在 Φ 上有超越基 B 而 P 在 Φ 上有超越基 B'，使 B^s, B'' 是不相交的，$B^s \cup B''$ 是代数无关的，则 (Γ, s, t) 是 E/Φ 和 P/Φ 的自由合成．

还要注意，如果对于 B 和 B'，引理的条件成立，则 $B^s \cup B''$ 是 Γ 的超越基．因为 E^s 与 P^t 的元均为 $\Phi(B^s \cup B'')$ 上的代数元，而 Γ 是由 E^s 和 P^t 生成的，因此 Γ 在 $\Phi(B^s \cup B'')$ 上是代数的，所以 $B^s \cup B''$ 是一个超越基．

我们可以用引理的判别方法去证明 Φ 上任意两个域 E 与 P 的自由合成的存在性．令 B 和 B' 分别是 Φ 上 E 和 P 的超越基．如果 B 和 B' 是有限的，即 $B=\{\xi_1, \cdots, \xi_m\}$，$B'=\{\eta_1, \cdots, \eta_n\}$，那末构造 $m+n$ 个未定元 $x_1, x_2, \cdots, x_{m+n}$ 的多项式代数 $\Phi[x_1, x_2, \cdots, x_{m+n}]$，并作它的分式域 $\Phi(x_1, x_2, \cdots, x_{m+n})$，我们有 $\Phi(B)$ 到 $\Phi(x_1, x_2, \cdots, x_{m+n})$ 内的同构使 $\xi_i \to x_i$ $(i=1, 2, \cdots, m)$ 及 $\Phi(B')$ 到 $\Phi(x_1, x_2, \cdots, x_{m+n})$ 内的同构 t 使 $\eta_j \to x_{m+j}$ $(j=1, 2, \cdots, n)$．现令 Ω 是 $\Phi(x_1, x_2, \cdots, x_{m+n})$ 的代数闭包，

那末我们知道，同构 s 与 t 分别可以开拓为 $\Phi(B)$ 与 $\Phi(B')$ 的代数扩张 E 与 P 到 Ω 内的同构 s 和 t（参考本章第一节习题中的第 1 题）. 由引理可知，如果 Γ 是由 E^s 和 P^t 生成的 Ω 的子域，则 (Γ, s, t) 是 E 和 P 的自由合成. 若 B 或 B' 是无限的，那末可以使用类似的步骤，或对此稍作修改，定义 B 和 B' 到其中基数较大的一个（比方说 B）内的 1-1 映射，使所得的象是不相交的，这些映射可以分别开拓为 $\Phi[B]$ 和 $\Phi[B']$ 内的同构 s 和 t. 则也能开拓为 $\Phi(B)$ 和 $\Phi(B')$ 到 $\Phi(B)$ 内的同构 s 和 t，从而能够开拓为 E 和 P 到 $\Phi(B)$ 的代数闭包 Ω 内的同构 s 和 t. 于是 (Γ, s, t) 是 P 和 E 的自由合成，这里 Γ 是由 E^s 和 P^t 生成的.

现在推广 § 1.16 的想法，得到 Φ 上两个给定域 E 和 P 的所有合成及所有自由合成（等价意义下）的概貌. 如前作张量积 $E\otimes_\Phi P$. 把 E 和 P 与它们在 $E\otimes_\Phi P$ 中的象等同起来. 令 $\mathfrak{P}$ 是 $E\otimes_\Phi P$ 的素理想（卷 1 的中译本 p. 160）；因此 $(E\otimes_\Phi P)/\mathfrak{P}$ 不仅是一个整区，而且是 Φ 上的一个代数. 我们可以把它嵌入其分式域 Γ 中. 设 s 表示 $E(\subseteq E\otimes P)$ 到 $(E\otimes_\Phi P)/\mathfrak{P}$ 的自然同态 $\varepsilon\to\varepsilon+\mathfrak{P}$. 因为 E 是域，$1^s=1$，所以这是一个同构. 还因为 $(E\otimes_\Phi P)/\mathfrak{P}\subseteq\Gamma$，可以把 s 看作是 E/Φ 到 Γ/Φ 内的同构. 类似地，有 P 到 Γ 内的同构 $t:\rho\to\rho+\mathfrak{P}$. 令 E 和 P 生成 $E\otimes P$，于是 E^s 和 P^t 生成代数 $(E\otimes P)/\mathfrak{P}$. 因为 Γ 是 $(E\otimes P)/\mathfrak{P}$ 的分式域，可见域 Γ 是由它的子域 E^s 和 P^t 生成的，故 (Γ, s, t) 是 E/Φ 和 P/Φ 的合成.

其次，设 $\mathfrak{P}'$ 是 $E\otimes_\Phi P$ 中另一个素理想，(Γ', s', t') 是按刚才所给方式构造的相应的合成. 设 (Γ', s', t') 和 (Γ, s, t) 等价，则有 Γ 到 Γ' 上的同构 u 使 $s'=su$，$t'=tu$，那么 u 映射为

$$\varepsilon^s=\varepsilon+\mathfrak{P}\to\varepsilon^{s'}=\varepsilon+\mathfrak{P}',\ \rho^t=\rho+\mathfrak{P}\to\rho+\mathfrak{P}'.$$

于是 u 在子代数 $E^sP^t/\mathfrak{P}$ 上的限制映射使 $\Sigma\varepsilon_i\rho_i+\mathfrak{P}\to\Sigma\varepsilon_i\rho_i+\mathfrak{P}'$，这里 $\varepsilon_i\in E$，$\rho_i\in P$. 因而与 § 1.16 一样，由 $\Sigma\varepsilon_i\rho_i\in\mathfrak{P}$ 推出 $\Sigma\varepsilon_i\rho_i\in\mathfrak{P}'$. 因此 $\mathfrak{P}\subseteq\mathfrak{P}'$ 而且如果对 u^{-1} 重复这个论证，得到 $\mathfrak{P}'\subseteq\mathfrak{P}$. 可见 $E\otimes_\Phi P$ 中不同的素理想给出 E/Φ 和 P/Φ 不等价的合

成.

今设 (Γ', s', t') 是 E/Φ 和 P/Φ 的任意合成，那末能把 E/Φ 和 P/Φ 到 Γ' 内的同构 s', t' 组合起来得到 $E\otimes_\Phi P$ 到 Γ' 内的同态：$\Sigma\varepsilon_i\rho_i \to \Sigma\varepsilon_i''\rho_i''$. 这个同态象是由 E''/Φ 和 P''/Φ 生成的子代数 $E''P''$. 这是一个整区. 因此如果 $\mathfrak{P}$ 是同态核，则

$$(E\otimes P)/\mathfrak{P} \cong E''P'',$$

而且 $(E\otimes P)/\mathfrak{P}$ 是一个整区. 因此 $\mathfrak{P}$ 是 $E\otimes P$ 的素理想，并可由此按前面方法构造合成 (Γ, s, t). 从 $E\otimes P$ 到 $E''P''$ 上的同态导出 $(E\otimes P)/\mathfrak{P}$ 到 $E''P''$ 上的同构使 $\Sigma\varepsilon_i\rho_i+\mathfrak{P}\to\Sigma\varepsilon_i''\rho_i''$. 这可唯一开拓为 $(E\otimes P)/\mathfrak{P}$ 的分式域 Γ 到 Γ' 上的同构 u. 我们有 $\varepsilon^{tu}=(\varepsilon+\mathfrak{P})^u=\varepsilon^{s'}, \varepsilon\in E$, $\rho^{tu}=(\rho+\mathfrak{P})^u=\rho^{t'}$, $\rho\in P$. 因此 u 是 (Γ, s, t) 和 (Γ', s', t') 的一个等价映射. 我们的讨论建立了 $E\otimes_\Phi P$ 的素理想 $\mathfrak{P}$ 的集到 E/Φ 和 P/Φ 的合成的等价类集间的 1-1 满射.

在 §1.16 中，我们建立了 $E\otimes_\Phi P$ (这里 $[P:\Phi]<\infty$) 的极大理想的集与 E/Φ 和 P/Φ 的合成的等价类间 1-1 满射. 我们现在看到那是现在所讨论的一种特殊情形. 我们知道，一个整区如果是有限维代数，则它是一个域(导言 p.8). 由此又可推出，有限维代数的任何素理想必是极大理想. 如果 P/Φ 是有限维的，则 $E\otimes_\Phi P$ 可以看作是 E 上的有限维代数，因此这个代数中的素理想是极大的. 对于 $[P:\Phi]<\infty$ 的情形，现在的对应就简化为前面的论断.

还剩下要把 $E\otimes P$ 中的、能使对应的合成 (Γ, s, t) 是自由的那些素理想找出来. 设 B 和 B' 分别是 E 和 P 的超越基. 我们知道 $\beta\in B$ 的单项式集 M 是 Φ 无关的. 对 $\beta'\in B'$ 的单项式集 M' 有类似的结论. 此外，若 $M=\{m_i\}$, $M'=\{n_j\}$, 则积的集 $\{m_in_j\}$ 是 Φ 无关的. 这就推得集 B 和 B' 是不相交的，而且 $B\cup B'$ 是一个代数无关集. 关于象 $B^t=\{\beta+\mathfrak{P}\}$ 和 $B''=\{\beta'+\mathfrak{P}\}$ 有相同结论成立当且仅当在 $E\otimes P$ 到 $(E\otimes P)/\mathfrak{P}$ 的自然同态下子代数 $\Phi[B\cup B']$ 没有非零元映射为 0. 这等价于条件

$$\Phi[B \cup B'] \cap \mathfrak{P} = 0.$$

因此得到了第一个条件：$E \otimes P$ 的素理想 $\mathfrak{P}$ 决定的合成 (Γ, s, t) 是自由合成当且仅当 $\Phi[B \cup B'] \cap \mathfrak{P} = 0$. 为了方便，我们常将这些条件稍作修改，即用 E 和 P 各自的子域 $\Phi(B)$ 和 $\Phi(B')$ 生成的子代数 $\Phi(B)\Phi(B')$ 来代替 $\Phi[B \cup B']$. 容易看出，$E \otimes P$ 的这些子代数的元有 $\mathrm{P}q^{-1}r^{-1}$ 形，这里 $\mathrm{P} \in \Phi[B \cup B']$，$q \in \Phi[B]$，$r \in \Phi[B']$. 显然 $\Phi[B \cup B']$ 是一个整区. 由此及 $\Phi(B)\Phi(B')$ 的元的形式推出 $\Phi(B)\Phi(B')$ 是一个整区. 若 $\mathrm{P}q^{-1}r^{-1} \neq 0$ 且属于 $\mathfrak{P} \cap \Phi(B)\Phi(B')$，则 $\mathrm{P} \neq 0$ 而且 $\mathrm{P} \in \Phi(B)\Phi(B') \cap \mathfrak{P}$. 因此

$$\mathfrak{P} \cap \Phi(B)\Phi(B') \neq 0$$

推出 $\mathfrak{P} \cap \Phi[B \cup B'] \neq 0$. 反之显然. 以上条件给出以下结论

引理 2. 由 $E \otimes P$ 的素理想 $\mathfrak{P}$ 定义的合成域 (Γ, s, t) 是自由的当且仅当 $\mathfrak{P} \cap \Phi(B)\Phi(B') = 0$，此处 B 和 B' 分别是 E/Φ 和 P/Φ 的超越基.

我们记得，如果 $\mathfrak{o}$ 是一个交换环，$\mathfrak{S}$ 是一个子环，则元 $a \in \mathfrak{o}$ 称为在 $\mathfrak{S}$ 上是整的，假若存在首项系数为 1 的多项式 $g(x) \in \mathfrak{S}[x]$，使 $g(a) = 0$（卷 1 的中译本 p. 168）. 我们曾经在卷 1 的 p. 169 证明了：如果 $\mathfrak{S}$ 是诺特环，则 $\mathfrak{o}$ 的 $\mathfrak{S}$ 整元集是一个包含 $\mathfrak{S}$ 的子环. 稍后会看到，这个结果对任何交换整区 $\mathfrak{o}$ 也是成立的. 但是诺特环这个条件对于证明以下所需结果是足够的.

引理 3. 设 B 和 B' 分别是 E/Φ 和 P/Φ 的超越基，则 $E \otimes_\Phi P$ 的每个元在 $\Phi(B)\Phi(B')$ 上都是整的.

证　因为 E 和 P 分别在 $\Phi(B)$ 和 $\Phi(B')$ 上是代数的. 显然 E 和 P 的元在 $\Phi(B)\Phi(B')$ 上是整的. 因为 $E \otimes P$ 由 E 和 P 生成，故只要证明 $\Phi(B)\Phi(B')$ 整元集是一个子环就行了，因此必须证明：当 α, β 是 $\Phi(B)\Phi(B')$ 整元时，$\alpha - \beta$ 和 $\alpha\beta$ 也是 $\Phi(B)\Phi(B')$ 整元. 因为任何一对元 α, β 在子代数 $\Phi(F)\Phi(F')$ 上都是整的，这里 F 和 F' 是 B 和 B' 的有限子集. 所以要证明 α, β 是 $\Phi(B)\Phi(B')$ 整元，只需对 B 和 B' 都是有限集来证明这一点就行了. 此时可以应用多项式环（卷 1 的中译本 p.159）的希尔伯特基定理推

出 $\Phi(B)[B']$ 是诺特环．下面证明 $\Phi(B)\Phi(B')$ 是诺特环．令 $\mathfrak{I}$ 是 $\Phi(B)\Phi(B')$ 的一个理想，则 $\mathfrak{I}'=\mathfrak{I}\cap\Phi(B)\Phi[B']$ 是 $\Phi(B)[B']$ 的理想，所以它有有限生成元集 $P_1, P_2, \cdots, P_m$. $\Phi(B)\Phi(B')$ 的任何元形为 Pq^{-1}，这里 $P\in\Phi(B)[B']$，$q\in\Phi[B']$. 如果这个元在 $\mathfrak{I}$ 内，则 $P=(Pq^{-1})q\in\mathfrak{I}'$，且 $P=\sum A_iP_i$，此处 $A_i\in\Phi(B)[B']$. 因此 $Pq^{-1}=\Sigma(A_iq^{-1})P_i$. 这就证明了 $P_1, P_2, \cdots, P_m$ 是 $\mathfrak{I}$ 的生成元集．所以 $\Phi(B)\Phi(B')$ 是诺特环．于是 $\alpha-\beta$ 和 $\alpha\beta$ 是 $\Phi(B)\Phi(B')$ 整的．证毕．

现在证明以下

定理 25. 由 $E\otimes_\Phi P$ 的素理想 $\mathfrak{P}$ 决定的 Φ 上的 E 和 P 的合成 (Γ, s, t) 是自由合成当且仅当 $\mathfrak{P}$ 的一切元均为 $E\otimes_\Phi P$ 的零因子．

证　根据引理 2 须证：对 E/Φ 和 P/Φ 的超越基 B 和 B'，$\mathfrak{P}$ 满足

$$\mathfrak{P}\cap\Phi(B)\Phi(B')=0$$

当且仅当 $\mathfrak{P}$ 的每个元都是零因子．首先假设 $\mathfrak{P}$ 只含零因子，且设 $P\in\mathfrak{P}\cap\Phi(B)\Phi(B')$，则 P 是 $\Phi(B)\Phi(B')$ 的元，且是 $E\otimes P$ 的零因子．我们要证 P 是 $\Phi(B)\Phi(B')$ 的零因子．为此，选取 E 在 $\Phi(B)$ 上的基 $\{u_\alpha\}$ 和 P 在 $\Phi(B')$ 上的基 $\{v_\beta\}$，容易看到，$E\otimes P$ 的每个元能写成和式 $\Sigma Q_{\alpha\beta}u_\alpha v_\beta$，$Q_{\alpha\beta}\in\Phi(B)\Phi(B')$. 而且

$$\Sigma Q_{\alpha\beta}u_\alpha v_\beta=0$$

仅当每个 $Q_{\alpha\beta}=0$（留作习题）．因为 P 是 $E\otimes P$ 的零因子，则存在元 $\Sigma Q_{\alpha\beta}u_\alpha v_\beta\neq0$ 使 $P(\Sigma Q_{\alpha\beta}u_\alpha v_\beta)=0$，即 $\Sigma PQ_{\alpha\beta}u_\alpha v_\beta=0$. 但因 $PQ_{\alpha\beta}\in\Phi(B)\Phi(B')$，故有 $PQ_{\alpha\beta}=0$ 而且有某些 $Q_{\alpha\beta}\neq0$，故 P 是 $\Phi(B)\Phi(B')$ 的一个零因子．因为 $\Phi(B)\Phi(B')$ 是整区，这就推出 $P=0$，所以 $\mathfrak{P}\cap\Phi(B)\Phi(B')=0$. 反之，假设

$$\mathfrak{P}\cap\Phi(B)\Phi(B')=0,$$

令 P 是 $\mathfrak{P}$ 的任一元，则由引理 3 推出：存在形如 $P^n+c_1P^{n-1}+c_2P^{n-2}+\cdots+c_n=0$ 的关系式，这里 $c_i\in\Phi(B)\Phi(B')$. 可以假设 n 是极小的．这个关系表明

$$c_n = -P^n - c_1P^{n-1} - \cdots - c_{n-1}P \in \mathfrak{P} \cap \Phi(B)\Phi(B'),$$

故 $c_n = 0$. 从而得到 $P(P^{n-1} + c_1P^{n-2} + \cdots + c_{n-1}) = 0$. 因为 n 是极小的，故 $P^{n-1} + c_1P^{n-2} + \cdots + c_{n-1} \neq 0$，则 P 是一个零因子. 故证明了任何 $P \in \mathfrak{P}$ 都是零因子. 证毕.

交换环 $\mathfrak{o}$ 的幂零元集形成一个理想称为 $\mathfrak{o}$ 的(诣零)根 $\mathfrak{N}$ (卷1的中译本 p. 161). 如果 $\mathfrak{P}$ 是 $\mathfrak{o}$ 的素理想，$z \in \mathfrak{N}$，则有整数 m 使 $z^m \in \mathfrak{P}$. 这就推出 $z \in \mathfrak{P}$. 所以 $\mathfrak{N}$ 包含于 $\mathfrak{o}$ 的每一素理想中[1]. 上节曾经证明，若 E 是 Φ 上的任意域，而且 Φ 在 P 中是可分代数封闭的，则 $E \otimes_\Phi P$ 的零因子是幂零元. 由此及刚才所指出的结果得到：$E \otimes P$ 的根 $\mathfrak{N}$ 是 $E \otimes_\Phi P$ 中元全为零因子的唯一素理想. 根据定理25以及 E 和 P 在 Φ 上的每一合成等价于由 $E \otimes P$ 的素理想所确定的某个合成这一事实，得到下列结果

定理 26. 设 E 是 Φ 的任意扩张域，Φ 在 P 中是可分代数封闭的，则在等价意义下，E/Φ 和 P/Φ 仅有一个自由合成.

---

1) 在第五章会看到，$\mathfrak{N}$ 是 $\mathfrak{o}$ 的所有素理想的交. ——著者注.

第五章
赋值论

域的赋值概念起源于人们希望给域的元赋予一个数量的想法．经典的例子是实数域或有理数域中的绝对值 $|\alpha|$．在有理数域和更一般的数域（有理数的有限代数扩张）的算术性质研究中，具有基本意义的是有理数域的 p-adic 赋值．对于给定的素数 p，有理数 α 的赋值 $\varphi_p(\alpha)$表示整除有理数 α 的 p 的幂．在代数函数域的研究中赋值也起着重要的作用．对此，必须稍微推广这一概念，使之等价于位的概念，而位的概念是由戴得金和韦伯（Weber）首先引入的，用来在代数函数中给出黎曼（Riemann）曲面的纯代数定义．赋值论已成为代数和分析之间的牢固的纽带：一方面，它加深了代数函数的研究，另一方面，它又导致引入分析的概念（如收敛性、积分）来研究数论的问题．

我们将从实数值赋值开始讨论，我们可区分两种类型：阿基米得（Archimedean）赋值和非阿基米得赋值．后者导致赋值概念的扩充，使其值不是取自实数域而是取自一个有序的交换群．我们将决定域的最简单形式的赋值，并较详细地考虑赋值的扩张问题．作为应用，将证明希尔伯特（Hilbert）零点定理，并研究交换整区的整闭包．

1. 实赋值 我们首先考虑取实数值的赋值，并称之为实赋值．在展开此理论的同时从收敛性的观点出发展开实数系是可能的，但会变得复杂些，因此，我们将不这样做而假定读者熟悉所需要的那部分有关实数的基本概念．

定义 1. 域 Φ 的一个**实赋值** φ 是 Φ 到实数域内的一个映射 $\alpha\to\varphi(\alpha)$，使得

(i) $\varphi(\alpha) \geqslant 0, \varphi(\alpha) = 0$ 当且仅当 $\alpha = 0$.

(ii) $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

(iii) $\varphi(\alpha + \beta) \leqslant \varphi(\alpha) + \varphi(\beta)$.

例. (1) Φ 为复数域，$\varphi(\alpha)$ 为通常的绝对值 $\sqrt{a^2+b^2}$，这里复数 $\alpha = a + b\sqrt{-1}$，a, b 为实数．这就给出了任意子域上的赋值，特别是实数域和有理数域上的赋值．

(2) Φ 为有理数域，p 为素数．若 $\alpha \neq 0, \alpha \in \Phi$，记 $\alpha = \alpha' p^k, k = 0, \pm 1, \pm 2, \cdots$，而 α' 是一个与 p 互素的有理数(记为：$(\alpha', p) = 1$)，所谓 α' 与 p 互素是指 α' 的某个表达式中的分子、分母均与 p 互素．整数 k 由 α 唯一决定，并记 $\nu_p(\alpha) = k$，$\varphi_p(\alpha) = p^{-\nu_p(\alpha)}$．此外，规定 $\nu_p(0) = \infty, \varphi_p(0) = 0$，则 (i) 是明显的，(ii) 和 (iii) 是正确的．若 $\alpha = 0$ 或 $\beta = 0$，这是显然的；设 $\alpha \neq 0, \beta \neq 0$ 且 $\alpha = \alpha' p^k$，$\beta = \beta' p^l$，其中 $(\alpha', p) = 1 = (\beta', p)$，则 $\alpha\beta = \alpha'\beta' p^{k+l}$ 和 $(\alpha'\beta', p) = 1$，因此 $\nu_p(\alpha\beta) = k + l = \nu_p(\alpha) + \nu_p(\beta)$，于是 $\varphi_p(\alpha\beta) = \varphi_p(\alpha)\varphi_p(\beta)$．如果 $k \leqslant l$，则 $\alpha + \beta = p^k(\alpha' + \beta' p^{l-k})$ 且 $\nu_p(\alpha + \beta) \geqslant \min(\nu_p(\alpha), \nu_p(\beta))$，因此 $\varphi_p(\alpha + \beta) \leqslant \max(\varphi_p(\alpha), \varphi_p(\beta))$，这个不等式是比(iii)更强的关系．于是 $\varphi_p(\alpha)$ 是个赋值，此赋值称为有理数域上 *p-adic* 赋值．

(3) $P = \Phi(x)$ 是 Φ 关于超越元 x 的扩张域，$\pi(x)$ 是 $\Phi[x]$ 内的不可约多项式．如果 α 是一个非零的有理式，记 $\alpha = \pi(x)^k \alpha'$，其中 k 为整数，α' 为有理式且与 π 互素($(\alpha', \pi) = 1$)，就是说，α' 有这样的表达式，其分子、分母均与 π 互素．令 $\nu_\pi(\alpha) = k$，$\varphi_\pi = c^k$(c 为实数，$0 < c < 1$)，并令 $\nu_\pi(0) = \infty, \varphi_\pi(0) = 0$．与例题中的(2)一样可验证 φ_π 是个赋值．这种类型赋值的典型情形是 Φ 为复数域，$\Phi(x)$ 为 Φ 上的有理函数域，这时 $\pi(x)$ 有形式 $x - r$，而 $\nu_\pi(\alpha(x))$ 刻划有理函数 $\alpha(x)$ 在点 $x = r$ 的邻域里的特性．我们看到：如果 $\nu_\pi(\alpha) = k > 0$，则 α 在 r 处有 k 阶的零点；如果 $\nu_\pi(\alpha) = -k, k > 0$，则 $\alpha(x)$ 在 $x = r$ 处有 k 阶的极点；如果 $\nu_\pi(\alpha) = 0$，则 α 在 $x = r$ 处既没有零点也没有极点．在无穷远点考虑 $\alpha(x)$ 的特性也是有趣的，这只要在 $\Phi(x)$ 中引进另外的赋值就可以做到：如果 $\alpha(x) \neq 0$，记 $\alpha(x) = (\beta_0 + \beta_1 x + \cdots + \beta_m x^m) \cdot (\gamma_0 + \gamma_1 x + \cdots + \gamma_n x^n)^{-1}$，其中 $\beta_m \neq 0, \gamma_n \neq 0$，则 $\alpha(x) = \left(\frac{1}{x}\right)^{n-m}\left(\beta_0\left(\frac{1}{x}\right)^m + \cdots + \beta_m\right)\left(\gamma_0\left(\frac{1}{x}\right)^n + \gamma_1\left(\frac{1}{x}\right)^{n-1} + \cdots + \gamma_n\right)^{-1}$，且若 $n - m > 0$，$\alpha(x)$ 在无穷远点有 $n - m$ 阶的零点，若 $n - m < 0$，$\alpha(x)$ 在无穷远点有 $m - n$ 阶的极点，如果 $n = m$，$\alpha(x)$ 在无穷远点既没有零点也没有极点．我们规定 $\nu_\infty(\alpha(x)) = n - m, \varphi_\infty(\alpha(x)) = c^{n-m}(0 < c < 1)$，$\nu_\infty(0) = \infty, \varphi_\infty(0) = 0$．这就给出了一个赋值．这种程序可应用于任何的 $\Phi(x)$(x 是超越元)．

(4) 对任意域 Φ，规定：当 $\alpha \neq 0$ 时，$\varphi(\alpha) = 1$；$\varphi(0) = 0$．此类赋值称为平凡的．我们特别指出例题(3)中的赋值 φ_π 和 φ_∞ 关于 Φ 均是平凡的．

今列出实赋值定义的某些直接推论：首先，由 (ii) 得到 $\varphi(1)$

$=1, \varphi(-1)=1$ 和 $\varphi(-\alpha)=\varphi(\alpha)$. 而且，如果 $\alpha\neq 0, \varphi(\alpha^{-1})=\varphi(\alpha)^{-1}$；如果 ζ 为单位根，$\varphi(\zeta)=1$. 由此得到，对有限域其仅有的赋值是平凡的. 我们还注意到

$$(1) \qquad |\varphi(\alpha)-\varphi(\beta)|\leqslant\varphi(\alpha-\beta),$$

其中 $|\ |$ 是普通的绝对值. 所有这些断言都是容易得到的，我们把证明留给读者.

定义 2. 实赋值 φ_1 和 φ_2 称为*等价的*，如果对 $\alpha,\beta\in\Phi$，$\varphi_1(\alpha)>\varphi_1(\beta)$ 当且仅当 $\varphi_2(\alpha)>\varphi_2(\beta)$.

从 §4 中我们要考察的收敛性的观点看，把具有上述定义那样关系的赋值视为恒同是很自然的. 此种关系导致了下述多少有点令人惊异的结论.

定理 1. 如果 φ_1 等价于 φ_2，则存在正实数 s 使得对一切 $\alpha\in\Phi$，$\varphi_2(\alpha)=\varphi_1(\alpha)^s$.

证. 由于断言中的 φ_1 和 φ_2 是对称的 $(\varphi_1=\varphi_2^{s^{-1}})$，我们可设 φ_1 和 φ_2 中的一个(例如 φ_1)是非平凡的，则存在 $\alpha_0\in\Phi$，使得 $0<\varphi_1(\alpha_0)<1=\varphi_1(1)$，因此，$0<\varphi_2(\alpha_0)<1$，故 φ_2 也是非平凡的，而且我们可记 $\varphi_2(\alpha_0)=\varphi_1(\alpha_0)^s$，其中 $s>0$. 事实上，此关系等价于 $s=\log\varphi_2(\alpha_0)/\log\varphi_1(\alpha_0)$，由于 $\log\varphi_2(\alpha_0)<0$，$\log\varphi_1(\alpha_0)<0$，故 $s>0$. 如果 α 是 Φ 中的任意元素，使得 $0<\varphi_1(\alpha)<1$，那么 $0<\varphi_2(\alpha)<1$，我们要证明

$$(2) \qquad \frac{\log\varphi_2(\alpha)}{\log\varphi_2(\alpha_0)}=\frac{\log\varphi_1(\alpha)}{\log\varphi_1(\alpha_0)}.$$

(2)中的两个比是正的. 令 m 和 n 是正整数，使得 $m/n>\log\varphi_1(\alpha)/\log\varphi_1(\alpha_0)$，则 $m\log\varphi_1(\alpha_0)<n\log\varphi_1(\alpha)$，$\log\varphi_1(\alpha_0^m)<\log\varphi_1(\alpha^n)$ 且 $\varphi_1(\alpha_0^m)<\varphi_1(\alpha^n)$. 因此，$\varphi_2(\alpha_0^m)<\varphi_2(\alpha^n)$，于是，如果，重复上述步骤，就得到 $m/n>\log\varphi_2(\alpha)/\log\varphi_2(\alpha_0)$，则 $m/n>\log\varphi_1(\alpha)/\log\varphi_1(\alpha_0)$. 由于对一切正有理数 $r=m/n$ 这些关系均能保持，故有等式(2). 因此

$$\frac{\log\varphi_2(\alpha)}{\log\varphi_1(\alpha)}=\frac{\log\varphi_2(\alpha_0)}{\log\varphi_1(\alpha_0)}=s,$$

且对一切的 α，使 $\varphi_1(\alpha)<1$，有 $\varphi_2(\alpha)=\varphi_1(\alpha)^s$。如果 $\varphi_1(\alpha)>1$，则取 α^{-1}后此等式仍成立。此外，如果 $\varphi_1(\alpha)=1=\varphi_1(1)$，则显然有 $\varphi_2(\alpha)=1$。因此，对一切 $\alpha,\varphi_2(\alpha)=\varphi_1(\alpha)^s$。

定义 3. 一个实赋值 φ 称为阿基米得赋值，如果对素域中的某个整数 $n(=n\cdot 1=1+1+\cdots+1,n$ 个 1)有 $\varphi(n)>1$。否则，此赋值称为非阿基米得的。

如果 Φ 有特征 $p\neq 0$，则素域中任何 $n\neq 0$ 均是单位根；因此 $\varphi(n)=1$。于是，特征为 p 的域的每个赋值都是非阿基米得的。我们也注意到，满足 $\varphi(\alpha+\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta))$ 的任何赋值是非阿基米得的。因为由归纳法可将此不等式推广为 $\varphi(\alpha_1+\alpha_2+\cdots+\alpha_n)\leqslant\max(\varphi(\alpha_1),\cdots,\varphi(\alpha_n))$，并由此得 $\varphi(n)\leqslant\varphi(1)=1$。此结果的逆也是正确的，因为有

定理 2. 如果 φ 是一个非阿基米得实赋值，则对 Φ 中每个 $\alpha,\beta,\varphi(\alpha+\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta))$。

证 我们有

$$\begin{aligned}\varphi(\alpha+\beta)^n&=\varphi(\alpha^n+\tbinom{n}{1}\alpha^{n-1}\beta+\cdots+\beta^n)\\&\leqslant\varphi(\alpha)^n+\varphi(\alpha)^{n-1}\varphi(\beta)+\cdots+\varphi(\beta)^n\\&\leqslant(n+1)\max(\varphi(\alpha)^n,\varphi(\beta)^n).\end{aligned}$$

因此，我们得到 $\varphi(\alpha+\beta)\leqslant(n+1)^{1/n}\max(\varphi(\alpha),\varphi(\beta))$。由于 $\lim\limits_{n\to\infty}(n+1)^{1/n}=1$，由此得

$$\varphi(\alpha+\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta)).\tag{3}$$

习 题 35

本习题中的"赋值"均指"实赋值"。

1. 证明：如果 φ 是一个赋值，s 是实数，$0<s<1$，则 $\alpha\to\varphi(\alpha)^s$是赋值。再证：如果 φ 是非阿基米得的，则对任何的 $s>0,\alpha\to\varphi(\alpha)^s$ 是赋值。

2. 建立非阿基米得赋值的下述性质：

(4) 如果 $\varphi(\alpha)>\varphi(\beta)$，则 $\varphi(\alpha+\beta)=\varphi(\alpha)$。

(5) 如果 $\alpha_1+\alpha_2+\cdots+\alpha_n=0$，则对某个 $i\neq j,\varphi(\alpha_i)=\varphi(\alpha_j)$。

3. 设 φ 为 P 的一个赋值，它在 P 的子域 Φ 上是平凡的，而 P 在 Φ 上是代数的，证明 φ 在 P 上是平凡的。

4. 设 φ 是 Φ 的非平凡赋值，β 是 Φ 的一个使 $\varphi(\beta)<1$ 的非零元，证明：$\varphi(\alpha)\leqslant 1$

当且仅当 $\varphi(\beta\alpha^n)<1$ $(n=1,2,\cdots)$. 由此证明：如果ψ是一个使得由 $\varphi(\gamma)<1$ 可推出 $\psi(\gamma)<1$ 的赋值，则也可由 $\varphi(\gamma)>1$ 得出 $\psi(\gamma)>1$，由 $\varphi(\gamma)=1$ 得出 $\psi(\gamma)=1$. 进而证明φ和ψ是等价的.

5. 证明：如果 $\varphi_1,\varphi_2,\cdots,\varphi_n$ 是域Φ上不等价的非平凡赋值，则存在α属于Φ使得 $\varphi_1(\alpha)>1$，而 $\varphi_i(\alpha)<1$，对 $i=2,3,\cdots,n$(提示：$n=2$ 的情形是第4题的一个简单推论. 用这个推论和归纳法可得到β使得 $\varphi_1(\beta)>1$, $\varphi_j(\beta)<1$; $j=1,2,\cdots,n-1$，而且以致于γ使得 $\varphi_1(\gamma)>1,\varphi_n(\gamma)<1$. 如果 $\varphi_n(\beta)\leqslant 1$，可对一个充分大的整数 k，取 $\alpha=\beta^k\gamma$. 如果 $\varphi_n(\beta)>1$，可对充分大的 k，取 $\alpha=\gamma\beta^k(1+\beta^k)^{-1}$).

2. 有理数域的实赋值 我们来决定有理数的阿基米得赋值. 其结果如下

定理 3. 有理数的任何阿基米得赋值等价于绝对值赋值.

证(阿廷) 设 n 和 n' 是大于1的整数，记 $n'=a_0+a_1n+\cdots+a_kn^k$, $0\leqslant a_i<n$, $a_k\neq 0$，则

$$\varphi(n')\leqslant\varphi(a_0)+\varphi(a_1)\varphi(n)+\cdots+\varphi(a_k)\varphi(n)^k.$$

由于 $0\leqslant\varphi(a_i)\leqslant a_i<n$，从而得到

$$\varphi(n')<n(1+\varphi(n)+\cdots+\varphi(n)^k)<$$
$$<n(k+1)\max(1,\varphi(n)^k).$$

我们有 $n'\geqslant n^k$，因此 $k\leqslant\log n'/\log n$，且

$$\varphi(n')<n\left(\frac{\log n'}{\log n}+1\right)\max(1,\varphi(n)^{\log n'/\log n}). \tag{6}$$

如果用 $(n')^r$ 代替 n'，r 为正整数，则从(6)得到

$$\varphi(n')^r<n\left(\frac{r\log n'}{\log n}+1\right)\max(1,\varphi(n)^{r\log n'/\log n}).$$

取 r 次根，得到

$$\varphi(n')<\left[n\left(\frac{r\log n'}{\log n}+1\right)\right]^{1/r}\max(1,\varphi(n)^{\log n'/\log n}). \tag{7}$$

由于 $a\neq 0$ 时，$\lim\limits_{r\to\infty}(ra+b)^{1/r}=1$，由(7)得

$$\varphi(n')\leqslant\max(1,\varphi(n)^{\log n'/\log n}). \tag{8}$$

由于φ是阿基米得赋值，可选 n'使得 $\varphi(n')>1$；因此由(8)得

$$1<\varphi(n')\leqslant\varphi(n)^{\log n'/\log n}. \tag{9}$$

因此 $\varphi(n)>1$，那么我们能交换 n 和 n' 的地位得到：对任何两个正整数 n 和 n'都有

(10) $$\varphi(n)^{1/\log n}=\varphi(n')^{1/\log n'},$$
故 $\log\varphi(n)/\log n$ 是一个与 n 无关的正实数 s 且 $\varphi(n)=n^s$. 于是，对每个有理数 α 有 $\varphi(\alpha)=|\alpha|^s$. 显然 $\varphi(\alpha)$ 等价于绝对值赋值.

定理 4. 有理数的任何非平凡非阿基米得实赋值等价于对某个素数 p 的 p-adic 赋值.

证 因对每个整数 n 有 $\varphi(n)\leqslant 1$. 若对每个整数，$\varphi(n)=1$,则 φ 是平凡的. 故存在非零整数 b 使得 $\varphi(b)<1$. 设 $\mathfrak{P}$ 是满足此条件的整数 b 的集,则此集为整数环 I 的一个理想,这是由于如果 $b_i\in\mathfrak{P}$ 有 $\varphi(b_1-b_2)\leqslant\max(\varphi(b_1),\varphi(b_2))$成立,如果 $n\in I$, $b\in\mathfrak{P}$ 有 $\varphi(nb)=\varphi(n)\varphi(b)<1$ 成立. 因此 $\mathfrak{P}=(p)$,这里 p 是一个素数. 由于 $0<\varphi(p)<1$, 故可表为 $\varphi(p)=p^{-s}$, 这里 $s>0$. 设 n 是任一整数,且使 $n=n'p^k$,这里 $k\geqslant 0,(n',p)=1$. 则 $n'\notin\mathfrak{P}$,那么 $\varphi(n')=1$; 因此 $\varphi(n)=p^{-ks}$. 由此得出 φ 是由 p 决定的 p-adic 赋值的 s 次幂.

3. $\Phi(x)$ 在Φ内为平凡的实赋值 设 x 是 $\mathrm{P}=\Phi(x)$ 的超越元,我们来决定 Φ 上的平凡的实赋值 φ. 由于素域包含在 Φ 内，对素域中每个整数$\neq 0$ 有 $\varphi(n)=1$, 因此 φ 是非阿基米得的.我们分两种情况讨论:

I. $\varphi(x)\leqslant 1$. 在此情况下,对每个$f(x)=\alpha_0+\alpha_1x+\cdots+\alpha_nx^n\in\Phi[x]$, $\varphi(f(x))\leqslant 1$. 由 φ 的非阿基米得性这是显然的. 从现在起假设 φ 是非平凡的，这意味着存在多项式 $f(x)$ 使得 $\varphi(f)<1$,设 $\mathfrak{P}$ 是 $\Phi[x]$ 的子集,$\mathfrak{P}$ 的元是使 $\varphi(f)<1$ 的多项式 f. 与定理 4 的证明一样可知 $\mathfrak{P}$ 是 $\Phi[x]$ 的素理想, $\mathfrak{P}=(\pi(x))$,且 $\varphi(\pi(x)),=c,0<c<1$.如果 $f(x)=\pi(x)^kg(x),(\pi(x),g(x))=1$,则 $\varphi(f)=c^k$. 因此 φ 是在§1 例题的(3)中讨论过的那个赋值 φ_π.

II. $\varphi(x)>1$. 设 $f(x)=\alpha_0+\alpha_1x+\cdots+\alpha_mx^m$, 其中 $\alpha_m\neq 0$. 则 $\varphi(\alpha_mx^m)=\varphi(x)^m>\varphi(\alpha_ix^i)$(对 $i<m$). 因此，$\varphi(f)=\varphi(x)^m$ (参看§1 习题中的第 2 题). 如果令 $\varphi(x)=c^{-1},0<c$

<1,则 $\varphi(f)=c^{-m}$. 容易验证 φ 是在 §1 例题的(3)中所定义的那个赋值 φ_∞.

4. 域的完备化 实赋值最重要的作用之一是替域引进度量空间的概念. 为此,最方便的方式是从序列和收敛性出发,其基本的定义是模仿普通分析学的.

定义 4. 设 Φ 是一个有实赋值 φ 的域,称序列 $\{\alpha_k\}$, $k=1$, $2,\cdots$ 在 Φ 中收敛(关于 φ),如果存在 $\alpha\in\Phi$,对任何实数 $\varepsilon>0$,存在整数 $N=N(\varepsilon)$,使得对一切 $n\geqslant N$ 有

$$(11)\qquad \varphi(\alpha-\alpha_n)<\varepsilon.$$

此时 α 是唯一的且称 α 为 $\{\alpha_k\}$ 的极限. 若 $\alpha=0$,$\{\alpha_k\}$ 叫做零序列. 序列 $\{\alpha_k\}$ 称为柯西 (Cauchy) 序列,如果对任意 $\varepsilon>0$,存在一个整数 $N=N(\varepsilon)$,使得对一切 $m,n\geqslant N(\varepsilon)$ 有

$$(12)\qquad \varphi(\alpha_m-\alpha_n)<\varepsilon.$$

级数 $\sum_1^\infty a_k$ 的收敛与通常一样,定义为部分和 $s_k=\sum_1^k a_i$ 的序列 $\{s_k\}$ 的收敛. 例如,在有 p-adic 赋值的有理数域内,由于当 n 充分大时,

$$\varphi_p\left(\frac{1}{1-p}-s_n\right)=\varphi_p(p^n)/\varphi_p(1-p)=p^{-n}<\varepsilon,$$

故级数 $\sum_1^\infty p^{k-1}$ 收敛于 $1/(1-p)$.

如同实数的情形,容易看出,任何收敛序列是柯西序列;反之不一定对. 这就导致有下述结论

定义 5. 称域 Φ 关于实赋值 φ 是完备的,如果 Φ 之元素的每个柯西序列在 Φ 中收敛.

对任何有实赋值 φ 的域 Φ,我们将着手构造 Φ 的完备化 $\bar{\Phi}$.此域 $\bar{\Phi}$ 有下述性质:

1. $\bar{\Phi}$ 是 Φ 的扩张域,有实赋值 $\bar{\varphi}$ 为 Φ 的赋值 φ 的一个扩张.

2. $\bar{\Phi}$ 是 $\bar{\varphi}$ 完备的.

3. 子域 Φ 在 $\bar{\Phi}$ 中是稠密的,也就是说: $\bar{\Phi}$ 的每个元均是 Φ 的

某个收敛序列的极限。

首先考虑 $\alpha_k \in \Phi$ 的柯西序列 $\{\alpha_k\}$ 的集 C。将证明 C 关于运算 $\{\alpha_k\} + \{\beta_k\} = \{\alpha_k + \beta_k\}, \{\alpha_k\}\{\beta_k\} = \{\alpha_k\beta_k\}$ 是一个环。为了今后的需要，有下述结论：

引理 1. 如果 $\{\alpha_k\}, \{\beta_k\} \in C$，则 $\{\alpha_k + \beta_k\}$ 和 $\{\alpha_k\beta_k\} \in C$。如果 $\{\alpha_k\} \in C$ 且为非零序列，则存在 $\eta > 0$ 和一个整数 N 使得 $\varphi(\alpha_n) > \eta$ 对一切 $n \geqslant N$ 成立。

证　给定 $\varepsilon > 0$，则存在 N_1 使得当 $m, n \geqslant N_1$ 时 $\varphi(\alpha_m - \alpha_n) < \varepsilon/2$，存在 N_2 使得当 $p, q \geqslant N_2$ 时 $\varphi(\beta_p - \beta_q) < \varepsilon/2$。设 $N = \max(N_1, N_2)$，则当 $m, n \geqslant N$ 时，$\varphi(\alpha_m + \beta_m - \alpha_n - \beta_n) \leqslant \varphi(\alpha_m - \alpha_n) + \varphi(\beta_m - \beta_n) < \varepsilon/2 + \varepsilon/2 = \varepsilon$。因此 $\{\alpha_k + \beta_k\} \in C$。其次，存在正实数 s, t 使得对一切 k 有 $\varphi(\alpha_k) < s$ 和 $\varphi(\beta_k) < t$；因为，如果当 N 充分大，$m \geqslant N$ 时，$\varphi(\alpha_m - \alpha_N) < 1$，故对一切的 $m \geqslant N$，有 $\varphi(\alpha_m) - \varphi(\alpha_N) \leqslant \varphi(\alpha_m - \alpha_N) < 1$，于是 $\varphi(\alpha_m) < \varphi(\alpha_N) + 1$。那么，如果 $s = \max(\varphi(\alpha_i) + 1)$，$i = 1, 2, \cdots, N$，则对一切 k，$\varphi(\alpha_k) < s$。类似地，我们能找到 $t > 0$，对一切 k，$\varphi(\beta_k) < t$。因此

$$
\begin{aligned}
(13) \qquad \varphi(\alpha_m\beta_m - \alpha_n\beta_n) &= \varphi(\alpha_m\beta_m - \alpha_m\beta_n + \alpha_m\beta_n - \alpha_n\beta_n) \\
&\leqslant \varphi(\alpha_m)\varphi(\beta_m - \beta_n) + \varphi(\beta_n)\varphi(\alpha_m - \alpha_n) \\
&< s\varphi(\beta_m - \beta_n) + t\varphi(\alpha_m - \alpha_n).
\end{aligned}
$$

如果取 N_1，使得对 $m, n \geqslant N_1$，$\varphi(\beta_m - \beta_n) < \varepsilon/2s$，取 N_2，使得对 $m, n \geqslant N_2$，$\varphi(\alpha_m - \alpha_n) < \varepsilon/2t$，则(13)表明，当 $m, n \geqslant N = \max(N_1, N_2)$ 时，$\varphi(\alpha_m\beta_m - \alpha_n\beta_n) < \varepsilon$。因此，$\{\alpha_k\beta_k\} \in C$。现设 $\{\alpha_k\} \in C$ 且不是零序列，则存在 $\varepsilon > 0$，使得对无限多个 k，$\varphi(\alpha_k) > \varepsilon$，并存在一个 N 使得对一切 $m, n \geqslant N$，$\varphi(\alpha_m - \alpha_n) < \varepsilon/2$。存在 $p \geqslant N$ 使得 $\varphi(\alpha_p) > \varepsilon$。因此，当 $n \geqslant p$ 时，$\varphi(\alpha_n) = \varphi(\alpha_p - (\alpha_p - \alpha_n)) \geqslant \varphi(\alpha_p) - \varphi(\alpha_p - \alpha_n) > \varepsilon/2 = \eta$。证毕。

欲证对已指出的运算 C 是一个环，我们只需回忆 Φ 的无穷序列的集关于分量加法和乘法作成环，此环恰是可数个 Φ 的完全直

和，此环的0元是$\{0\}$，单位元是$\{1\}$，用$\{\alpha\}$表示当$k=1,2,3,\cdots$时，$\alpha_k=\alpha$的序列$\{\alpha_k\}$，并称这样的序列为**常量序列**$\{\alpha\}$．显然，常量序列的集是序列环的一个子环，且在映射$\alpha\to\{\alpha\}$之下同构于Φ．由引理1可知柯西序列的集C是序列环的子环，显然C包含常量序列环．因此，C是一个交换环，有单位元$1=\{1\}$，且C包含同构于Φ的常量序列环为子环．

其次，考虑C的由零序列组成的子集Z，我们有下述结论

引理2． Z是C的一个极大理想．

证　易知两个零序列的差$\{\alpha_k\}-\{\beta_k\}=\{\alpha_k-\beta_k\}$是零序列．现设$\{\alpha_k\}$为零序列，$\{\gamma_k\}$为柯西序列，引理1的证明表明，存在正实数$s$使得对一切$k$，$\varphi(\gamma_k)<s$．如果$\varepsilon>0$，选择$N$使得对一切$n\geqslant N$有$\varphi(\alpha_n)<\varepsilon/s$，则$\varphi(\alpha_n\gamma_n)<\varepsilon$，对一切$n\geqslant N$．于是$\{\alpha_k\gamma_k\}$是一个零序列，因此$Z$是$C$的一个理想．为了证明$Z$是极大理想我们要证明两件事：$Z\neq C$且如果$B$是$C$中包含$Z$的任一理想，且含一个元$\{\gamma_k\}\notin Z$，则$B=C$．由于$Z$中不包含任何$\neq\{0\}$的常量序列，第一点是明显的．其次，设$B$是一个$C$中包含$Z$的理想，且含有元$\{\alpha_k\}\notin Z$，引理1表明存在正数$\eta$和整数$p$使得对一切$n\geqslant p$，$\varphi(\alpha_n)>\eta$．令$\beta_k=1$，如果$k<p$；$\beta_k=\alpha_k$，如果$k\geqslant p$．则$\{\alpha_k\}-\{\beta_k\}\in Z$．考虑序列$\{\beta_k^{-1}\}$，我们有

$$\varphi(\beta_m^{-1}-\beta_n^{-1})=\frac{1}{\varphi(\beta_m\beta_n)}\varphi(\beta_m-\beta_n)<\frac{1}{\eta^2}\varphi(\alpha_m-\alpha_n),$$

如果$m,n\geqslant p$．由此得$\{\beta_k^{-1}\}\in C$．由于$\{\alpha_k\}-\{\beta_k\}\in Z\subseteq B$，$\{\alpha_k\}\in B$，$\{\beta_k\}\in B$，由此$1=\{\beta_k^{-1}\}\{\beta_k\}\in B$，于是$B=C$．

由引理2得差环$\bar{\Phi}=C/Z$是一个域．我们继续证$\bar{\Phi}$是一个具有赋值的域，而且是Φ的完备化．

定理5． 设Φ是一个有实赋值φ的域，$\bar{\Phi}=C/Z$为柯西序列环关于零序列理想Z的差环，则$\bar{\Phi}$是一个域，且包含一个子域同构于Φ，如果使Φ等同于此子域，则$\bar{\Phi}$是Φ的一个完备化．

证　我们知道映射$\alpha\to\{\alpha\}$是Φ和C的一个子环的同构．由于Z中的常量序列只能是$\{0\}$，所以自然同态$\{\alpha\}\to\{\alpha\}+Z$是

一个同构，因此，得到Φ到 $\bar{\Phi}=C/Z$ 内的同构 $\alpha\to\{\alpha\}+Z$。从现在起我们将把α和 $\{\alpha\}+Z$、Φ 和它在 $\bar{\Phi}$ 内的象等同起来。下面我们证明 $\bar{\Phi}$ 有一个赋值 $\bar{\varphi}$ 是Φ之赋值φ的一个扩充。设$\{\alpha_k\}\in C$。由于 $|\varphi(\alpha_m)-\varphi(\alpha_n)|\leqslant\varphi(\alpha_m-\alpha_n)$ 和 $\{\alpha_k\}$ 是柯西序列，则 $\{\varphi(\alpha_k)\}$是一个实数柯西序列。因此，由实数域关于绝对赋值的完备性知道 $\lim\varphi(\alpha_k)$ 存在。其次令$\{\alpha'_k\}$是另外的柯西序列使 $\{\alpha_k\}+Z=\{\alpha'_k\}+Z$。这意味着对给定的 $\varepsilon>0$，如果 $n\geqslant N(\varepsilon)$ 有 $\varphi(\alpha_n-\alpha'_n)<\varepsilon$。于是 $|\varphi(\alpha_n)-\varphi(\alpha'_n)|<\varphi(\alpha_n-\alpha'_n)<\varepsilon$，如果 $n\geqslant N(\varepsilon)$。因此，$\lim\varphi(\alpha_k)=\lim\varphi(\alpha'_k)$，故这个实数与陪集$A=\{\alpha_k\}+Z$ 中的元$\{\alpha_k\}$之选择无关。现在令$\bar{\varphi}(A)=\lim\varphi(\alpha_k)$ 并着手证明 $\bar{\varphi}$ 是 $\bar{\Phi}$ 的一个赋值。首先 $\bar{\varphi}(A)\geqslant 0$ 是显然的。如果 $A=\{\alpha_k\}+Z$ 和 $\bar{\varphi}(A)=0$，则 $\lim\varphi(\alpha_k)=0$；因此 $\{\alpha_k\}$ 是零序列，那么 $\{\alpha_k\}\in Z$ 和 $A=0$。如果 $B=\{\beta_k\}+Z$，则 $AB=\{\alpha_k\beta_k\}+Z$，$\bar{\varphi}(AB)=\lim\varphi(\alpha_k\beta_k)=\lim\varphi(\alpha_k)\varphi(\beta_k)=\bar{\varphi}(A)\bar{\varphi}(B)$。又 $A+B=\{\alpha_k+\beta_k\}+Z$ 和 $\bar{\varphi}(A+B)=\lim\varphi(\alpha_k+\beta_k)\leqslant\lim(\varphi(\alpha_k)+\varphi(\beta_k))=\bar{\varphi}(A)+\bar{\varphi}(B)$。因此 $\bar{\varphi}$ 是一个赋值。如果 $A=\alpha\in\Phi$，那么 $A=\{\alpha\}+Z$，则 $\bar{\varphi}(A)=\lim\varphi(\alpha)=\varphi(\alpha)$；因此 $\bar{\varphi}$ 是Φ的赋值φ的一个扩张。其次将证明Φ在 $\bar{\Phi}$ 内稠密。设 $A=\{\alpha_k\}+Z$ 是 $\bar{\Phi}$ 的一个元，α'_k 是常量序列，其一切项均为 α_k，则我们将 $A_k=\alpha'_k+Z$ 等同于 α_k。我们断言 $\lim A_k=A$。因为，如果给定 $\varepsilon>0$，则能找到N使得 $\varphi(\alpha_m-\alpha_n)<\varepsilon$，若 $m,n\geqslant N$。则 $\lim\limits_{n\to\infty}\varphi(\alpha_m-\alpha_n)$ 存在且 $\leqslant\varepsilon$。另一方面，$\bar{\varphi}(A-A_m)=\lim\limits_{n\to\infty}\varphi(\alpha_m-\alpha_n)$，故 $\bar{\varphi}(A-A_m)\leqslant\varepsilon$，若 $m\geqslant N$。因此，$\lim A_k=A$ 且Φ在 $\bar{\Phi}$ 内是稠密的。最后要证明 $\bar{\Phi}$ 是完备的：设$\{A_k\}$是 $\bar{\Phi}$ 的一个柯西序列。对每个 k，可以选择 $\alpha_k\in\Phi\subseteq\bar{\Phi}$ 使得$\bar{\varphi}(A_k-\alpha_k)<\frac{1}{2^k}$，则 $\varphi(\alpha_m-\alpha_n)=\bar{\varphi}(\alpha_m-A_m+A_m-A_n+A_n-\alpha_n)\leqslant\bar{\varphi}(\alpha_m-A_m)+\bar{\varphi}(A_m-A_n)+\bar{\varphi}(A_n-\alpha_n)\leqslant\bar{\varphi}(A_m-A_n)+\frac{1}{2^m}+\frac{1}{2^n}$。由于$\{A_k\}$是一

个柯西序列，这就证明了 $\{\alpha_k\}$ 是 Φ 的一个柯西序列．现在如果回到原来的 Φ 并取元 $A=\{\alpha_k\}+Z$，α_k 在原来的 Φ 中，那么易知 $\lim A_k=A$．

从现在起将仍用 φ 记 $\bar{\Phi}$ 中的赋值 $\bar{\varphi}$．

现在着手处理域 $\bar{\Phi}$ 的唯一性问题．更一般地，设 $\bar{\Phi}_i, i=1, 2$，是具有赋值 φ_i 的完备域，Φ_i 是稠密子域．设 s 是一个 Φ_1 到 Φ_2 上的同构，它是等距的，即 $\varphi_2(\alpha^s)=\varphi_1(\alpha)$，$\alpha\in\Phi_1$．令 $A\in\bar{\Phi}_1$，$\{\alpha_k\}$是 Φ_1 的一个序列使得 $\lim\alpha_k=A$，则 $\{\alpha_k^s\}$是 Φ_2 中的一个柯西序列，于是它有极限 B．如果$\{\alpha_k'\}$是第二个序列，有$\lim\alpha_k'=A$，则$\lim(\alpha_k-\alpha_k')=0$，$\lim\varphi_1(\alpha_k-\alpha_k')=0$；因此，$\lim\varphi_2(\alpha_k^s-\alpha_k'^s)=0$，$\lim(\alpha_k^s-\alpha_k'^s)=0$．由此得$\lim\alpha_k'^s=B$．因此，$\bar{\Phi}_1$ 到 $\bar{\Phi}_2$ 内的映射 $\bar{s}$: $A\to B$ 是单值的，容易验证这是一个同态，显然在 Φ_1 上有 $\bar{s}=s$．类似的，用定义 $\bar{s}$ 的同样方法能把 s^{-1}扩充为 $\bar{\Phi}_2$ 到 $\bar{\Phi}_1$ 内同态 $\overline{s^{-1}}$．故对一切 $A\in\bar{\Phi}_1$ 有 $A^{\bar{s}\overline{s^{-1}}}=A$，而对一切 $B\in\bar{\Phi}_2$ 有 $B^{\overline{s^{-1}}\bar{s}}=B$．由此得 $\bar{s}$ 是满射，且是一个同构．最后注意到，如果 $\bar{s}_1$ 和 $\bar{s}_2$ 是 $\bar{\Phi}_1$ 到 $\bar{\Phi}_2$ 上的等距同构，且在 Φ_1 上重合，则 $\bar{s}_1=\bar{s}_2$．证明是显然的．因此有下述结论：

定理 6. 设 $\bar{\Phi}_i, i=1,2$，是一个完备域，具有赋值 φ_i，且 Φ_i 为 $\bar{\Phi}_i$ 的稠密子域．设 s 是 Φ_1 到 Φ_2 上的一个等距同构．则 s 能唯一地扩张为 $\bar{\Phi}_1$ 到 $\bar{\Phi}_2$ 上的一个等距同构．

特别，可由此得出：如果 $\bar{\Phi}_1$ 和 $\bar{\Phi}_2$ 是同一个域 Φ 的完备化，则存在一个 $\bar{\Phi}_1/\Phi$ 到 $\bar{\Phi}_2/\Phi$ 上的等距同构．这只要把此定理用到 Φ 内的恒等映射上就行了．在此意义上的完备化是唯一的并且我们可以使用术语：域 Φ 关于实赋值 φ 的完备化．

习　题　36

1．设 Φ 是一个域，具有实赋值 φ．证明在通常的意义下，和、差与积是 Φ 上的连续函数．并证明映射 $\alpha\to\alpha^{-1}$ 在 Φ^* 上是连续的，Φ^*是 Φ 的非零元集．

2．设 $\bar{\Phi}$ 是 Φ 的完备化．证明恒等映射是 $\bar{\Phi}$ 仅有的，在 Φ 上的连续自同构．

5. p-adic 数域的一些性质　我们首先注意任意域关于非平凡的非阿基米得实赋值 φ 的某些性质．如果 Φ 是这样一个域，则

Φ中使 $\varphi(\alpha)\leqslant 1$ 的元α所成的集$\mathfrak{o}$是Φ的一个子环；因为，如果 $\alpha,\beta\in\mathfrak{o}$,则 $\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)\leqslant 1$ 和 $\varphi(\alpha-\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta))\leqslant 1$. 称此环$\mathfrak{o}$为$\varphi$的**赋值环**. $\mathfrak{o}$中使 $\varphi(\beta)<1$ 的元β所成的子集$\mathfrak{p}$是$\mathfrak{o}$的一个理想,这是因为由 $\varphi(\beta_1)<1,\varphi(\beta_2)<1,\varphi(\alpha)<1$ 可推出 $\varphi(\beta_1-\beta_2)<1$ 和 $\varphi(\alpha\beta_1)<1$. 在$\mathfrak{o}$中但却不在$\mathfrak{p}$中的元α满足 $\varphi(\alpha)=1$;因此，$\varphi(\alpha^{-1})=1$ 且$\alpha^{-1}\in\mathfrak{o}$. 反之,如果$\alpha$是$\mathfrak{o}$中的一个单位,则由 $\varphi(\alpha)\leqslant 1$, $\varphi(\alpha^{-1})\leqslant 1$ 和 $\varphi(\alpha)\varphi(\alpha^{-1})=1$ 得出 $\varphi(\alpha)=1$, 于是 $\alpha\notin\mathfrak{p}$. 可见$\mathfrak{p}$是$\mathfrak{o}$中非单位的集. 由此得到,$\mathfrak{o}$中任一真含$\mathfrak{p}$的理想含有一个单位，因而与$\mathfrak{o}$重合. 故$\mathfrak{p}$是$\mathfrak{o}$中的极大理想. 若$\mathfrak{q}$是真含于$\mathfrak{o}$的任一理想,则$\mathfrak{q}$不含$\mathfrak{o}$的单位;所以，$\mathfrak{q}\subseteq\mathfrak{p}$. 因此，$\mathfrak{p}$是$\mathfrak{o}$的唯一的极大理想. 差环 $\mathfrak{o}/\mathfrak{p}$ 是一个域，称为Φ关于φ的**剩余域**.

显然,集 $\Gamma=\{\varphi(\alpha),\alpha\neq 0,\ \alpha\in\Phi\}$是正实数乘法群的一个子群,称$\Gamma$为$\varphi$的**值群**，如果$\Gamma$是一个循环群则称此赋值为**离散的**. 容易看出,正实数的子群 $\Gamma\neq 1$ 是循环的当且仅当<1的元的子集 Γ'有一个极大元. 此元是Γ的生成元. 设φ是离散的,π 是Φ的一个元,它在Γ内能使 $\varphi(\pi)$ 是<1的最大元,则$\pi\in\mathfrak{p}$, $\mathfrak{p}$ 为赋值环$\mathfrak{o}$的极大理想，而且如果 β是$\mathfrak{p}$的任意元素，则 $\varphi(\beta)\leqslant\varphi(\pi)$, $\varphi(\beta\pi^{-1})\leqslant 1$,于是 $\beta\pi^{-1}=\alpha\in\mathfrak{o}$, $\beta=\alpha\pi$. 故$\mathfrak{p}$是主理想(π). 反之,如果$\mathfrak{p}$是一个主理想: $\mathfrak{p}=(\pi)$,则任一 $\beta\in\mathfrak{p}$ 有形式 $\alpha\pi$, $\alpha\in\mathfrak{o}$,于是 $\varphi(\beta)=\varphi(\alpha)\varphi(\pi)\leqslant\varphi(\pi)$. 因此 $\varphi(\pi)$ 是Γ内<1的最大元而且φ是离散的.由于$\varphi(\pi)$是Γ的生成元，对Φ中任意非零的α有 $\varphi(\alpha)=\varphi(\pi)^k$,$k$ 为某个整数. 因此，若 $\varepsilon=\alpha\pi^{-k}$, $\varphi(\varepsilon)=\varphi(\alpha)\varphi(\pi)^{-k}=1$,则$\varepsilon$是$\mathfrak{o}$的一个单位,所以，$\Phi$的任一非零元形如 $\varepsilon\pi^k$, $k=0,\pm1,\pm2,\cdots$,其中ε是$\mathfrak{o}$的一个单位.

设Φ是任一有非阿基米得实赋值φ的域，$\bar{\Phi}$是Φ关于φ的完备化. 现在去证明，Φ和$\bar{\Phi}$的赋值群相同，并在某种意义下对剩余域也有相同的结论. 设 $\bar{\alpha}\in\bar{\Phi}$，则由$\Phi$在$\bar{\Phi}$内的稠密性得出:在$\Phi$中存在$\alpha$使得 $\varphi(\bar{\alpha}-\alpha)<\varphi(\bar{\alpha})$. 由于赋值是非阿基米得的,故有 $\varphi(\alpha)=\varphi(\bar{\alpha}+(\alpha-\bar{\alpha}))=\max(\varphi(\bar{\alpha}),\ \varphi(\alpha-\bar{\alpha}))=$

$\varphi(\bar{\alpha})$. 因此，有 $\alpha\in\Phi$ 使得 $\varphi(\alpha)=\varphi(\bar{\alpha})$，这显然表示 Φ 和 $\bar{\Phi}$ 有相同的值群 Γ. 次设 $\bar{\mathfrak{o}}$ 是 $\bar{\Phi}$ 的赋值环，$\bar{\mathfrak{p}}$ 是它的非单位的极大理想，如果 $\mathfrak{o}$ 和 $\mathfrak{p}$ 是 Φ 中相应的子集，则 $\mathfrak{o}=\bar{\mathfrak{o}}\cap\Phi$，$\mathfrak{p}=\bar{\mathfrak{p}}\cap\Phi$. 如果 $\bar{\alpha}\in\bar{\mathfrak{o}}$，选择 $\alpha\in\Phi$ 使得 $\varphi(\bar{\alpha}-\alpha)<1$，则 $\bar{\alpha}-\alpha\in\bar{\mathfrak{p}}$，于是 $\alpha\in\mathfrak{o}$，因此 $\bar{\alpha}\equiv\alpha(\bmod\bar{\mathfrak{p}})$，这就证明了 $\mathfrak{o}+\bar{\mathfrak{p}}=\bar{\mathfrak{o}}$. 我们有标准的同构：

$$\bar{\mathfrak{o}}/\bar{\mathfrak{p}}=(\mathfrak{o}+\bar{\mathfrak{p}})/\bar{\mathfrak{p}}\cong\mathfrak{o}/(\mathfrak{o}\cap\bar{\mathfrak{p}})=\mathfrak{o}/\mathfrak{p}.$$

借助这个同构，我们能把 $\bar{\Phi}$ 和 Φ 的剩余域等同起来.

在具有非阿基米得赋值的完备域中，级数收敛的理论特别简单. 由完备性推出，$\sum\limits_{1}^{\infty}\alpha_k$ 收敛当且仅当对任一 $\varepsilon>0$，存在一个整数 N 使得 $\varphi(\alpha_{m+1}+\cdots+\alpha_{m+k})<\varepsilon$，如果 $m\geqslant N$，而 $k=1,2,\cdots$. 由于赋值为非阿基米得的，$\varphi(\alpha_{m+1}+\cdots+\alpha_{m+k})\leqslant\max\varphi(\alpha_{m+i})$. 因此，此条件等价于 $\varphi(\alpha_{m+i})<\varepsilon$，对 $m\geqslant N$，$i=1,2,\cdots$. 而这就等价于 $\lim\alpha_n=0$. 这表明，一个级数收敛当且仅当它的第 n 项收敛于零. 由于 $\sum\limits_{1}^{\infty}\alpha_k=\sum\limits_{1}^{m}\alpha_i+\sum\limits_{m+1}^{\infty}\alpha_i$，得 $\varphi\left(\sum\limits_{1}^{\infty}\alpha_k\right)\leqslant\max\left(\varphi\left(\sum\limits_{1}^{m}\alpha_i\right),\varphi\left(\sum\limits_{m+1}^{\infty}\alpha_j\right)\right)$，由于把 m 取得充分大可以使 $\varphi\left(\sum\limits_{m+1}^{\infty}\alpha_j\right)$ 变得任意小，如果 m 充分大我们就有 $\varphi\left(\sum\limits_{1}^{\infty}\alpha_k\right)=\varphi\left(\sum\limits_{1}^{m}\alpha_i\right)$. 如果另外还有 $\varphi(\alpha_1)>\varphi(\alpha_2)>\varphi(\alpha_3)>\cdots$，则 $\varphi\left(\sum\limits_{1}^{m}\alpha_i\right)=\varphi(\alpha_1)$，因而，此时有 $\varphi\left(\sum\limits_{1}^{\infty}\alpha_k\right)=\varphi(\alpha_1)$.

现在考虑域 $\bar{R}^{(p)}$ 的特别情形，$\bar{R}^{(p)}$ 是有理数域 R_0 关于 p-adic 赋值 $\varphi_p(\alpha)=p^{-k}$ 的完备化，这里 $\alpha=p^k\alpha'$，$(\alpha',p)=1$. 称域 $\bar{R}^{(p)}$ 为 p-adic **数域**. 显然，R_0 关于 φ_p 的值群是由 p^{-1} 生成的循环群；因此对 $\bar{R}^{(p)}$ 有相同的结果，R_0 和 $\bar{R}^{(p)}$ 的赋值是离散的. 设 $\mathfrak{o}$ 是 $\bar{R}^{(p)}$ 的赋值环，$\bar{\mathfrak{o}}$ 的元是使 $\varphi_p(\bar{\alpha})\leqslant1$ 的 p-adic 数

$\bar{\alpha}$,这些数称为 p-adic 整数.由 φ_p 的定义显然可把是 p-adic 整数的有理数表示为 m/n,而 $(n,p)=1$. 若 $\mathfrak{o}$ 为 R_0 的赋值环,$\mathfrak{p}$ 为它的极大理想,则 $\mathfrak{o}=\bar{\mathfrak{o}}\cap R_0,\mathfrak{p}=\bar{\mathfrak{p}}\cap R_0$. 我们知道 $\bar{\mathfrak{o}}=\mathfrak{o}+\bar{\mathfrak{p}}$,因此,如果 $\bar{\alpha}$ 是任意 p-adic 整数,则存在有理数 $m/n,(n,p)=1$,使得 $\bar{\alpha}-m/n\in\bar{\mathfrak{p}}$,还存在整数 a,b 使 $na+pb=1$; $m/n=ma+p(bm/n)$, $m/n\equiv ma(\bmod\bar{\mathfrak{p}})$, 故 $\bar{\alpha}\equiv ma(\bmod\bar{\mathfrak{p}})$, 这表明 $\bar{\mathfrak{o}}=I+\bar{\mathfrak{p}}$,而 I 为整数环. 显然 $\bar{\mathfrak{p}}\cap I=(p)$,因此剩余域 $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}\cong I/(p)$ 恰好是 p 个元的域.

设 $\bar{\alpha}$ 为 p-adic 整数,则上述的讨论表明存在一个元 $a\in I$(即 a 是一个普通的整数), 使得 $\bar{\alpha}-a\in\bar{\mathfrak{p}}$. 如果 $a\equiv b(\bmod p)$, 则 $a-b\in\bar{\mathfrak{p}}$,则 $\bar{\alpha}-b\in\bar{p}$. 这说明,对每个 p-adic 整数 $\bar{\alpha}$, 能选择 $a_0\in\{0,1,2,\cdots,p-1\}$,使得 $\bar{\alpha}-a_0\in\bar{p}$, 我们断言 $\bar{\alpha}_1=\frac{1}{p}(\bar{\alpha}-a_0)$ 是一个 p-adic 整数. 首先, 注意 p 是 $\mathfrak{p}$ 中使 $\varphi(p)$ 为极大的元,由于 R_0 和 $\bar{R}^{(p)}$ 的值群相同, 故 p 为 $\bar{\mathfrak{p}}$ 中有极大 $\varphi(p)$ 的元. 所以,理想 $\bar{\mathfrak{p}}$ 是以 p 为生成元的主理想,于是, 如果 $\bar{\beta}$ 满足 $\varphi(\bar{\beta})<1$, 则 $\bar{\beta}=\gamma p$,而 γ 为一个 p-adic 整数. 特别, $\bar{\alpha}-a_0=p\bar{\alpha}_1$,其中 $\bar{\alpha}_1\in\bar{\mathfrak{o}}$. 因此 $\bar{\alpha}_1=\frac{1}{p}(\bar{\alpha}-a_0)\in\bar{\mathfrak{o}}$. 对 $\bar{\alpha}_1$ 重复这种讨论,就可找到 $a_1=0,1,2,\cdots,p-1$ 使得 $\bar{\alpha}_1-a_1\in\bar{\mathfrak{p}}$ 且 $\bar{\alpha}_2=\frac{1}{p}(\bar{\alpha}_1-a_1)\in\bar{\mathfrak{o}}$. 这样 $\bar{\alpha}=a_0+p\bar{\alpha}_1=a_0+a_1p+\bar{\alpha}_2p^2$. 如此继续下去得

$$\bar{\alpha}=a_0+a_1p+a_2p^2+\cdots+a_kp^k+\bar{\alpha}_{k+1}p^{k+1},$$

其中 $0\leqslant a_i\leqslant p-1,\bar{\alpha}_{k+1}\in\bar{\mathfrak{o}}$. 那么 $\bar{\alpha}_{k+1}p^{k+1}\to 0$, 故有

(14) $$\bar{\alpha}=a_0+a_1p+a_2p^2+\cdots,0\leqslant a_i\leqslant p-1.$$

反之,考虑这种形式的任一级数: 可设此级数为 $a_mp^m+a_{m+1}p^{m+1}+\cdots$,其中 $m\geqslant 0,a_m\neq 0$. 则此级数收敛. 如果 $\bar{\alpha}$ 是它的极限,则 $\varphi_p(\bar{\alpha})=\varphi_p(p^m)=p^{-m}$. 因此 $\bar{\alpha}\in\bar{\mathfrak{o}}$. 我们还知道,$\bar{\alpha}$ 是 $\bar{\mathfrak{o}}$ 的单位当且仅当 $m=0$. 故 $\bar{\mathfrak{o}}$ 的单位是使 $a_0\neq 0$ 的元(14),已

知理想 $\bar{\mathfrak{p}}$ 是由 p 生成的主理想．由此得 $\bar{R}^{(p)}$ 的每个元有形式 $p^k\varepsilon$，而 ε 是一个单位，$k=0$[1]，±1，±2，$\cdots$．因此每个元有形式 $p^k(a_0+a_1p+\cdots)$，其中 $0\leqslant a_i\leqslant p-1$．

设 U 是 $\bar{\mathfrak{o}}$ 中单位的乘法群，我们希望分析 U 的结构，首先要证明 U 含有一个子群同构于 $I/(p)$ 中非零元乘法群，即一个 $p-1$ 阶的循环群．设 a 为数 $1,2,3,\cdots,p-1$ 中的一个，则 $a^p=a+xp$，而 $x\in I$．由归纳法得 $a^{p^k}\equiv a^{p^{k-1}}(\bmod p^k)$，那么 $\dfrac{a^{p^k}-a^{p^{k-1}}}{p^k}\in I\subseteq\bar{\mathfrak{o}}$．由此可见

$$\zeta_a=a+\left(\frac{a^p-a}{p}\right)p+\left(\frac{a^{p^2}-a^p}{p^2}\right)p^2+\cdots \tag{15}$$

是 $\bar{R}^{(p)}$ 中一个完全确定的元，即序列 $\{\zeta_a^{(k)}\}$ 的极限，这里

$$\zeta_a^{(k)}=a+\left(\frac{a^p-a}{p}\right)p+\cdots+\left(\frac{a^{p^k}-a^{p^{k-1}}}{p^k}\right)p^k=a^{p^k}.$$

在任一个具有赋值的域中，如同实数域那样我们能证明由 $\lim a_k=\bar{\alpha},\lim b_k=\bar{\beta}$ 可得出 $\lim(a_k\pm b_k)=\bar{\alpha}\pm\bar{\beta}$ 和 $\lim a_kb_k=\bar{\alpha}\bar{\beta}$（参看§4，习题中的第1题）．因此，由 $\lim\zeta_a^{(k)}=\zeta_a$ 得出 $\lim(\zeta_a^{(k)})^p=\zeta_a^p$．由于 $\zeta_a^{(k)}=a^{p^k}$ 得 $\lim a^{p^k}=\zeta_a$ 和 $\lim(a^{p^k})^p=\lim a^{p^{k+1}}=\zeta_a^p$．然而，显然 $\lim a^{p^{k+1}}=\zeta_a$，故有 $\zeta_a^p=\zeta_a$．又由(15)易见 $\zeta_a\equiv a(\bmod\bar{\mathfrak{p}})$，并且因 $a\not\equiv0,(\bmod\bar{\mathfrak{p}})$，$\zeta_a\neq0$，于是 $\zeta_a^{p-1}=1$．同理可证，如果在集 $\{1,2,\cdots,p-1\}$ 中 $a\neq b$，则 $\zeta_a\neq\zeta_b$．因此，我们作出了 $p-1$ 个不同的 $p-1$ 次单位根．这就是在域中我们所能有的全部元．我们还知道 $\{\zeta_a\}$ 是一个循环群（§1.13，引理1）．

设 $\varepsilon\in U$，于是 $\varepsilon=a+a_1p+a_2p^2+\cdots$，其中 $0<a<p$，$0\leqslant a_i<p$，故 $\zeta_a\equiv\varepsilon(\bmod\bar{\mathfrak{p}})$，$\varepsilon_1=\zeta_a^{-1}\varepsilon\equiv1(\bmod\bar{\mathfrak{p}})$．如果一个 p-adic 整数模 $\bar{\mathfrak{p}}$ 同余于1，则称**1单位**（*Einseinheit*）．我们已证明 $\bar{\mathfrak{o}}$ 中每个单位形为 $\varepsilon=\varepsilon_1\zeta_a$，其中 ε_1 是一个1单位．设 U_1 是1单位的集，则 U_1 是 U 的子群．欲证之，可设 $\eta_1,\eta_2\in U_1$，那么 $\eta_i=1+\bar{\beta}_i$，$\bar{\beta}_i\in\bar{\mathfrak{p}}$，则由于 $\bar{\beta}_1+\bar{\beta}_2+\bar{\beta}_1\bar{\beta}_2\in\bar{\mathfrak{p}}$ 得 $\eta_1\eta_2=1+\bar{\beta}_1$

1) 原文误为1．——译者注．

$+\bar\beta_2+\bar\beta_1\bar\beta_2\equiv 1\pmod{\bar{\mathfrak p}}$. 也易知 $1-\bar\beta_1+\bar\beta_1^2-\cdots=(1+\bar\beta_1)^{-1}$. 显然，$1-\bar\beta_1+\bar\beta_1^2-\cdots\equiv 1\pmod{\bar{\mathfrak p}}$. 故 $\bar\eta_1^{-1}=(1+\bar\beta_1)^{-1}\in U_1$.

为了更严密地研究 U 的子群 U_1，在 p-adic 数域中引进指数函数最为方便，我们利用级数来定义它：

$$\exp x=1+\frac{x}{1!}+\frac{x^2}{2!}+\cdots, \tag{16}$$

我们要证明，当 $p\neq 2$ 时，此级数对一切 $x\in\bar{\mathfrak p}$ 是收敛的. 如同 §1 中一样，记 $\varphi_p(x)=p^{-\nu_p(x)}$，我们知道 $\nu_p(x)$ 是一个整数. 条件 $\nu_p(x)=l>0$ 等价于：$x\in\bar{\mathfrak p}^{-l}$. 对一个有理数来说，$\nu_p(x)$ 是 p 的幂，并在 $x=p^{\nu_p(x)}y,(y,p)=1$ 的意义下整除 x. 为了证明(16)的收敛性，我们显然需要一个关于 $\nu_p(k!)$ 的公式. 为此，我们注意到数 $1,2,3,\cdots,k$ 中有 $\left[\frac{k}{p}\right]$ 个可能被 p 整除，(这些是 p，$2p,3p,\cdots,\left[\frac{k}{p}\right]p.$)$[x]$ 表示实数 x 的整数部分. 类似的，数 $1,2,\cdots,k$ 中有 $\left[\frac{k}{p^2}\right]$ 个可能被 p^2 整除，$\left[\frac{k}{p^3}\right]$ 个可被 p^3 整除，等等. 这就得到

$$\nu_p(k!)=\left[\frac{k}{p}\right]+\left[\frac{k}{p^2}\right]+\left[\frac{k}{p^3}\right]+\cdots.$$

因此 $\nu_p(k!)<k\left(\frac{1}{p}+\frac{1}{p^2}+\cdots\right)=k\left(\frac{1}{p-1}\right)$. 我们现在设 $p\neq 2$，那么如果 $\nu_p(x)=l\geqslant 1$ 和 $k>0$ 则 $\nu_p(x^k/k!)>k\left(l-\frac{1}{p-1}\right)>0$. 取 $\nu_p(0)=\infty$，此式还可包括 $x=0$ 在内. 此不等式表明：若 $k>0$，则 $x^k/k!\in\bar{\mathfrak p}$ 而且 $\lim x^k/k!=0$，因此(16)是收敛的而且 $\exp x$ 对一切 $x\in\bar{\mathfrak p}$ 有定义. 此外，由于对 $k>0$，$x^k/k!\in\bar{\mathfrak p}$，则 $\exp$ 是 $\bar{\mathfrak o}$ 的一个元，$\exp x\equiv 1\pmod{\bar{\mathfrak p}}$，因此 $\exp x\in U_1$. 如果 $x\neq 0$ 和 $\nu_p(x)=l\geqslant 1$，则 $\nu_p(x^2/2!)=2l>$

l，且若 $k>2$，则 $\nu_p(x^k/k!)>k(l-1/(p-1))>l$。由此得到，如果 $x\in\mathfrak{p}^l$，$l\geqslant 1$，则

(17)
$$\exp x-1-x\in\mathfrak{p}^{l+1}.$$

现在将证明，如果 $x,y\in\mathfrak{p}$，则

(18)
$$\exp(x+y)=(\exp x)(\exp y).$$

设

$$X_n=\sum_0^n\frac{x^k}{k!}\ ,\ Y_n=\sum_0^n\frac{y^k}{k!}\ ,\ Z_n=\sum_0^n\frac{(x+y)^k}{k!}.$$

由于

$$\frac{1}{k!}(x+y)^k=\sum_{l=0}^k\frac{x^{l}y^{k-l}}{l!(k-l)!}$$

$$Z_{2n}-X_nY_n=\sum_{l+k\leqslant 2n\quad l>n\text{或}k>n}\frac{x^ly^k}{l!k!}.$$

由上面指出的不等式推出 $\lim(Z_{2n}-X_nY_n)=0$。由于 $\lim X_n=\exp x$，$\lim Y_n=\exp y$，$\lim Z_{2n}=\exp(x+y)$，这就得到(18)。等式(18)和 $\exp x\in U_1$ 可建立加群$(\mathfrak{p},+)$ 到 U_1 内的一个同态。我们将证明事实上映射 $x\to\exp x$ 是 $(\mathfrak{p},+)$到 U_1 上的同构。欲证此映射为同构，只需证明由 $x\neq 0$ 可推出 $\exp x\neq 1$即可。因此，设 $\nu_p(x)=l\neq\infty$，那么 $x\in\mathfrak{p}^l$，$x\notin\mathfrak{p}^{l+1}$。则由(17)显然可得 $\exp x\neq 1$。

其次考虑 U_1 的任一元，此元有形式 $1+y$，$y\in\mathfrak{p}$。令 $x_1=y$ 并考虑 $(1+y)\exp(-x_1)$，由(17)，$\exp(-x_1)=1-x_1+z_1$，其中 $z_1\in\mathfrak{p}^2$；因此

$$\begin{aligned}(1+y)\exp(-x_1)&=(1+x_1)(1-x_1+z_1)\\&=1+(z_1-x_1^2+x_1z_1)\\&=1+x_2,\end{aligned}$$

其中 $x_2=z_1-x_1^2+x_1z_1\in\mathfrak{p}^2$。设我们早已决定元素 $x_1,x_2,\cdots,x_k$ 使得 $x_i\in\mathfrak{p}^i$，且

---

1) 原文误为 x^k。—— 译者注.

$$(1+y)\exp(-x_1-x_2-\cdots-x_k)=1+x_{k+1}$$

其中 $x_{k+1}\in\bar{\mathfrak{p}}^{k+1}$,则

$$\begin{aligned}(1+y)&\exp(-x_1-x_2-\cdots-x_{k+1})\\&=(1+y)\exp(-x_1-x_2-\cdots-x_k)\exp(-x_{k+1})\\&=(1+x_{k+1})\exp(-x_{k+1})\\&=(1+x_{k+1})(1-x_{k+1}+z_{k+1}),\end{aligned}$$

其中 $z_{k+1}\in\bar{\mathfrak{p}}^{k+2}$,$(1+x_{k+1})(1-x_{k+1}+z_{k+1})=1+x_{k+2}$,这里 $x_{k+2}=z_{k+1}-x_{k+1}^2+x_{k+1}z_{k+1}\in\bar{\mathfrak{p}}^{k+2}$. 这表明对任一整数$n\geqslant 1$,存在 $x_1, x_2, \cdots, x_n$, $x_i\in\bar{\mathfrak{p}}^i$, 使得 $(1+y)\exp\left(-\sum_1^n x_i\right)\equiv 1(\mathrm{mod}\,\bar{\mathfrak{p}}^{n+1})$,故 $x=\sum_1^\infty x_k$ 是 $\bar{\mathfrak{p}}$ 的元,我们断言 $\exp x=1+y$.

设 $X_n=\sum_1^n x_i$,则由于 $X_n-x\in\bar{\mathfrak{p}}^{n+1}$ 得 $\exp(-x)\exp X_n=\exp(X_n-x)\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1})$. 如同对 $\bar{\mathfrak{p}}$ 一样我们可以验证: 如果 $z_1\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1})$,和 $z_2\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1})$. 则 $z_1z_2\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1})$. 因此,我们能从 $(1+y)\exp(-X_n)\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1})$ 和 $\exp(-x)\exp X_n\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1})$得结论

$$(1+y)\exp(-x)\equiv 1(\mathrm{mod}\ \bar{\mathfrak{p}}^{n+1}).$$

由于n是任意的,可得 $(1+y)\exp(-x)=1$ 和 $1+y=\exp x$ 如所需. 这表明 $x\to\exp x, x\in\bar{\mathfrak{p}}$, 是到 U_1 上的满射. 因此就证明了下述的结论

定理 7. 设 $\bar{\mathfrak{p}}$ 是 p-adic 整数环 $\bar{\mathfrak{o}}$ 的极大理想, $p\neq 2$, U_1 是元$\equiv 1(\mathrm{mod}\,\bar{\mathfrak{p}})$ 的群,则指数映射 $x\to\exp x$ 是加群 $(\bar{\mathfrak{p}},+)$到 $\bar{\mathfrak{o}}$ 的 1 单位乘法群 U_1 上的同构.

注. 要证 $x\to\exp x$ 是满射这一事实自然的方式是给出逆函数 $\log(1+y)=y-\frac{y^2}{2}+\frac{y^3}{3}-\cdots$,它对一切的 $y\in\bar{\mathfrak{p}}$ 有定义(下面习题中的第 4 题). 然后我们必须证明$\exp(\log(1+y))=$

$1+y$. 详细的证明是稍长了点. 为此,我们宁可采用上述方式证明 $x \to \exp x$ 是满射. 因为这样做不要求将它的逆定义为显函数. 对此问题的完整叙述，读者可参阅哈塞 (Hasse) 的《数论》(Zahlentheorie)，柏林，1949，pp. 188—199.

由定理 7 易见群 U_1 没有有限阶元,因此,如果 Z 表示前面已构作的 $(p-1)$ 次单位根的群，则 $U_1 \cap Z = 1$. 我们知道 $\bar{\mathfrak{o}}$ 的单位群 U 的每个元是 Z 的一个元和 U_1 的一个元的积,故 $U = U_1 \times Z$ (直积).

作为这些结果的一个应用，考虑在 p-adic 域中方程 $x^2 = m$ 的可解性问题,其中 m 为通常的整数,与 p 互素,$p \neq 2$. 则 $m \in U$ 且可写成 $m = \eta\zeta_a$,其中 $\eta \in U_1$, $m \equiv a(\mathrm{mod}\ p)$,$0 < a < p$. 显然,如果对 $\bar{a} \in \bar{R}^{(p)}$ 有 $\bar{a}^2 = m$,则 $\varphi_p(\bar{a}) = 1$,于是如果 $x^2 = m$ 在 $\bar{R}^{(p)}$ 中有解,则此解必属于 U,此解有形式 $\bar{\lambda}\zeta_b$,这里 ζ_b 是一个 $(p-1)$ 次单位根，$\bar{\lambda} \in U_1$. 从 $U = U_1 \times Z$ 得到 $\bar{\lambda}^2 = \eta$, $\zeta_b^2 = \zeta_a$. 我们指出对任一 $\eta \in U_1$,方程 $x^2 = \eta^2$ 恒有解. 利用 U_1 和 $(\bar{\mathfrak{p}}, +)$ 的同构，只需知道映射 $x \to 2x$ 是后一个群的自同构就行了. 由于 $2^{-1} \in U$,显然 $x \to 2^{-1}x$ 把 $\bar{\mathfrak{p}}$ 映射到自身且是映射 $x \to 2x$ 的逆. 由此可见: 方程 $x^2 = m$ 在 $\bar{R}^{(p)}$ 内可解当且仅当 $\zeta_b^2 = \zeta_a$ 是可解的. 易知对这个问题的条件是 $x^2 \equiv m$ 或 $x^2 \equiv a$ $(\mathrm{mod} p)$ 可解,即 m 是模 p 的二次剩余. 因此 $x^2 = m$ 在 $\bar{R}^{(p)}$ 内可解,$p \neq 2$,$(m, p) = 1$,当且仅当 $x^2 \equiv m(\mathrm{mod} p)$在整数中有解,即当且仅当$\left(\frac{m}{p}\right) = 1$,$\left(\frac{m}{p}\right)$是勒让得 (Legendre) 符号.

例如，如果 $p = 5$ 和$m = -1$，则 $2^2 \equiv -1(\mathrm{mod} 5)$，$\left(\frac{-1}{5}\right) = 1$,因此$\sqrt{-1}$ 在 5-adic 域中存在;另一方面,$\left(\frac{3}{5}\right) = -1$,因此 $\sqrt{3}$ 在此域中不存在.

习　题　37

1. 把 5-adic 整数 $\frac{2}{3}$ 表示为形如(14)的 5-adic 展开式.

2. 证明对任一个 $p=2,3,5,\cdots$, p-adic 数域是不可数的. 用此证明在有理数子域上超越的 p-adic 数的存在性.

3. 利用 $(1-2x)^{1/2}$ 的二项展开式在 5-adic 数域中得到 $\sqrt{-1}=\frac{1}{3}(1-10)^{1/2}$ 的一个收敛级数.

4. 定义 $\log(1+y)=y-\frac{y^2}{2}+\frac{y^3}{3}-\cdots$, 证明若 $p\neq 2$, 此级数对一切 $y\in\bar{\mathfrak{p}}$ 收敛. 证明 $\log(1+y_1)(1+y_2)=\log(1+y_1)+\log(1+y_2)$, $y_i\in\bar{\mathfrak{p}}$.

5. 证明方程 $x^3=4$ 在5-adic 数域中是可解的.

6. 证明在 2-adic 数域中, 指数映射是 $\bar{\mathfrak{p}}^2$ 到 $\mathfrak{o}$ 中 $\equiv 1(\bmod \bar{\mathfrak{p}}^2)$ 的元素所成的群上的同构.

6. 亨泽尔 (Hensel) 引理 有另外一个更有效的方法处理 p-adic 数域以及更一般的带离散非阿基米得实赋值的完备域中的方程, 这一方法是建立在多项式的基本可约性准则之上的, 它就是著名的

亨泽尔引理. 设 Φ 为关于一个非阿基米得离散实赋值 φ 的完备域, $\mathfrak{o}$ 是 Φ 的赋值环, $\mathfrak{p}$ 为 $\mathfrak{o}$ 的极大素理想, $\Delta=\mathfrak{o}/\mathfrak{p}$ 为剩余域, $\alpha\to\alpha^*=\alpha+\mathfrak{p}$ 是 $\mathfrak{o}$ 到 Δ 上自然同态. 设 $f(x)\in\mathfrak{o}[x]$ 有性质: 它在 $\Delta[x]$ 中的象 $f^*(x)=\gamma(x)\eta(x)$, 其中 $(\gamma(x),\eta(x))=1$ 且 $\gamma(x)$ 的首项系数为 1. 则在 $\mathfrak{o}[x]$ 中 $f(x)=g(x)h(x)$, 其中 $g^*(x)=\gamma(x)$, $h^*(x)=\eta(x)$, $\deg g(x)=\deg\gamma(x)$ 且 $g(x)$ 的首项系数为 1.

证　设 $\deg f(x)=n$, $\deg\gamma(x)=r\leqslant n$. 可选 $g_1(x),h_1(x)\in\mathfrak{o}[x]$ 使 $g_1^*(x)=\gamma(x)$, $h_1^*(x)=\eta(x)$, $\deg g_1(x)=r$, $\deg h_1(x)\leqslant n-r$, $g_1(x)$ 的首项系数为 1. 则在系数同余 $(\bmod\mathfrak{p})$ 的意义下得 $f(x)\equiv g_1(x)h_1(x)\ (\bmod\ \mathfrak{p})$. 在 $\mathfrak{o}[x]$ 中我们着手解决两个多项式序列 $\{g_k(x)\}$, $\{h_k(x)\}$, $k=1,2,\cdots$, 使得: (i) $g_k(x)\equiv g_{k+1}(x)\ (\bmod\ \mathfrak{p}^k)$, $h_k(x)\equiv h_{k+1}(x)(\bmod\ \mathfrak{p}^k)$, (ii) $f(x)\equiv g_k(x)h_k(x)\ (\bmod\ \mathfrak{p}^k)$, (iii) $\deg g_k(x)=r$, $\deg h_k(x)\leqslant n-r$, $g_k(x)$ 的首项系数

为 1. 这些序列可以从我们所选择的 $g_1(x)$ 和 $h_1(x)$ 开始. 因此可设对 $k \leqslant s$ 时序列已经作出. 我们令 $g_{s+1}(x) = g_s(x) + u(x)\pi^s, h_{s+1}(x) = h_s(x) + v(x)\pi^s$,其中 $\mathfrak{p} = (\pi)$ (同 §5),则 (i) 对在 $\mathfrak{d}[x]$ 中任意选择的 $u(x)$和 $v(x)$(i) 成立. 我们找出满足 (ii) 的,这就要求

$$\begin{aligned} f(x) &\equiv [g_s(x) + u(x)\pi^s][h_s(x) + v(x)\pi^s] \\ &\equiv g_s(x)h_s(x) + [g_s(x)v(x) + h_s(x)u(x)]\pi^s (\bmod\ \mathfrak{p}^{s+1}), \end{aligned}$$

或

$$(19) \qquad \begin{aligned} f(x) - g_s(x)h_s(x) \equiv [g_s(x)v(x) + \\ + h_s(x)u(x)]\pi^s (\bmod\ \mathfrak{p}^{s+1}). \end{aligned}$$

由于 $f(x) \equiv g_s(x)h_s(x) (\bmod\ \mathfrak{p}^s)$,则$f(x) - g_s(x)h_s(x) = \pi^s\omega(x)$,其中 $\omega(x) \in \mathfrak{d}[x]$. 由于 $\deg f(x) = n$ 和$\deg g_s(x)h_s(x) \leqslant n$,我们可设 $\deg\ \omega(x) \leqslant n$. 显然,如果

$$(20) \qquad g_s(x)v(x) + h_s(x)u(x) \equiv \omega(x) (\bmod \mathfrak{p}),$$

则(19)成立. 于是由(i),显然有 $g_s^*(x) = g_1^*(x) = \gamma(x)$和 $h_s^*(x) = \eta(x)$,那么在 $\Delta[x]$ 内考虑方程

$$(21) \qquad \gamma(x)v^*(x) + \eta(x)u^*(x) = \omega^*(x).$$

由于$(\gamma(x), \eta(x)) = 1$, 因此存在多项式 $\alpha(x)$, $\beta(x) \in \Delta[x]$ 使 $\alpha(x)\gamma(x) + \beta(x)\eta(x) = 1$,乘以 $\omega^*(x)$ 得到 $\kappa(x), \lambda(x)$使$\kappa(x)\gamma(x) + \lambda(x)\eta(x) = \omega^*(x)$. 我们能使 $\lambda(x) = \gamma(x)\mu(x) + \rho(x)$,而 $\deg\ \rho(x) < r$,故得

$$\begin{aligned} \omega^*(x) &= \kappa(x)\gamma(x) + (\gamma(x)\mu(x) + \rho(x))\eta(x) \\ &= (\kappa(x) + \mu(x)\eta(x))\gamma(x) + \rho(x)\eta(x). \end{aligned}$$

则当 $\deg\ \omega^*(x) \leqslant n$ 时,$\deg\ \rho(x)\eta(x) < n$. 由于 $\deg\gamma(x) = r$,上述关系表明 $\deg(\kappa(x) + \mu(x)\eta(x)) \leqslant n - r$. 我们记这个多项式为 $\sigma(x)$,则

$$\sigma(x)\gamma(x) + \rho(x)\eta(x) = \omega^*(x),$$

而 $\deg \rho(x) < r$,$\deg \sigma(x) \leqslant n - r$,则我们可在 $\mathfrak{D}[x]$中选出 $u(x)$ 和 $v(x)$使 $u^*(x) = \rho(x)$,$v^*(x) = \sigma(x)$,$\deg u(x) = \deg \rho(x) = r$,$\deg\ v(x) \leqslant n - r$,那么(21)成立且 $g_{s+1}(x) = g_s(x) + u(x)\pi^s$,

$h_{s+1}(x) =$ [1] $h_s(x) + v(x)x^s$ 还满足(iii). 这就完全证明了满足(i),(ii)和(iii)的序列$\{g_k(x)\}$,$\{h_k(x)\}$($k=1,2,\cdots$)的存在性. 由条件(i),(iii)和Φ的完备性推出序列$\{g_k(x)\}$,$\{h_k(x)\}$收敛于多项式$g(x)$,$h(x)$,多项式序列收敛的意义是指x的相同幂的系数序列收敛于$g(x)$,$h(x)$的同次幂的系数. 而且$\deg g(x) = r$,$\deg h(x) \leqslant n-r$,$g(x)$的首项系数为1. 又由(ii)得$f(x) = g(x)h(x)$. 证毕.

习 题 38

1. 利用亨泽尔引理证明,在 p-adic 数域中存在ξ_a使得$\xi_a^{p-1}=1$,$\xi_a \equiv a(\bmod \mathfrak{p})$其中$a$是任一个与$p$互素的整数. 并用此得出在5-adic 数域中存在$\sqrt{-1}$和$\sqrt[3]{4}$的另一证明.

2. 设Φ与亨泽尔引理中的一样. 令$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathfrak{o}[x]$,满足: $a_0, a_n \in \mathfrak{p}$,但存在$a_r$,$1 \leqslant r \leqslant n-1$,使$a_r \notin \mathfrak{p}$. 则$f(x)$在$\mathfrak{o}[x]$中是可约的. 用此证明,如果$g(x) = x^n + \alpha_1x^{n-1} + \cdots + \alpha_n$在$\Phi[x]$中的不可约多项式,$\alpha_n \in \mathfrak{o}$,则一切$\alpha_i \in \mathfrak{o}$.

7. 具有给定剩余域的完备域的构造 给定域Δ. 我们考虑构造具有非阿基米得实赋值的完备域使给定的域Δ为其剩余域. 我们将给出两个构造: 第一,在此构造中,完备域包含Δ并与Δ有相同的特征;第二,在此构造中,Δ是完备的,其特征$p \neq 0$,而该完备域的特征为0. 后者的一个特殊情形是$\Delta = I_p$,而完备域则是p-adic 数域.

首先考虑域$\Phi = \Delta(\xi)$,ξ是Δ上的超越元素. 我们用$\nu(\alpha(\xi)) = k$引进序函数ν,如果$\alpha(\xi) = \xi^k\beta(\xi)\gamma(\xi)^{-1}$,而$\beta(\xi)$和$\gamma(\xi)$是不能被$\xi$整除的多项式. 我们用$\varphi(\alpha(\xi)) = c^{\nu(\alpha(\xi))}$定义一个赋值$\varphi$,$c$是一个固定实数,$0<c<1$(参看§1,例题中的第3题). 令$\bar{\Phi}$是关于$\varphi$的$\Phi$之完备化. 由于$\varphi$在$\Delta$上是平凡的,显然$\varphi$是非阿基米得赋值,因此$\varphi$扩张到$\bar{\Phi}$上是非阿基米得的,仍用$\varphi$记之. Φ和$\bar{\Phi}$的值群是由c的幂组成的,故赋值是离散的.

---

1) 原文误为"+"——译者注.

令 $\bar{\mathfrak{o}}$ 是 $\bar{\Phi}$ 的赋值环，$\bar{\mathfrak{p}}$ 为其极大理想，并设 $\mathfrak{o}=\bar{\mathfrak{o}}\cap\Phi$，$\mathfrak{p}=\bar{\mathfrak{p}}\cap\Phi$，显然 ξ 是 $\bar{\mathfrak{p}}$ 的一个元且使 $\varphi(\xi)=c$ 为极大元．因此，如同 p-adic 数一样，$\bar{\Phi}$ 的每个元 α 有形式 $\xi^k\bar{\varepsilon}$，其中 $\bar{\varepsilon}\in\bar{\mathfrak{o}}$，$\notin\bar{\mathfrak{p}}$，而 k 是一个整数．故可定义 $\nu(\xi^k\bar{\varepsilon})=k$，显然这与原来在 Φ 中定义的序函数 ν 重合．

在§5 我们已有 $\bar{\mathfrak{o}}=\mathfrak{d}+\bar{\mathfrak{p}}$，这样允许我们可以等同剩余域 $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ 和 $\mathfrak{d}/\mathfrak{p}$．环 $\mathfrak{d}$ 是 ξ 的系数在 Δ 中且"在 0 处有限"的有理式的集，即 $\alpha(\xi)=\beta(\xi)\gamma(\xi)^{-1}$，其中 β，γ 为多项式且 $\gamma(0)\neq 0$．在 p-adic 数中证明 $\bar{\mathfrak{o}}=I+\bar{\mathfrak{p}}$ 的推理(p.218)能用于此处以证明 $\bar{\mathfrak{o}}=\Delta[\xi]+\bar{\mathfrak{p}}$．由于 $\xi\in\bar{\mathfrak{p}}$，这就给出 $\bar{\mathfrak{o}}=\Delta+\bar{\mathfrak{p}}$，且由于 $\bar{\mathfrak{p}}\cap\Delta=0$，我们得到 $\delta\to\delta+\bar{\mathfrak{p}}\in\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ 是 Δ 到剩余域 $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ 内的同构．在此意义下，可以说 Δ 是 $\bar{\Phi}$ 的剩余域．

现设 $\bar{\alpha}$ 为 $\bar{\mathfrak{o}}$ 的任一个元，则 $\bar{\mathfrak{o}}=\Delta+\bar{\mathfrak{p}}$ 表明能找到 $\delta_0\in\Delta$ 使得 $\bar{\alpha}-\delta_0\in\bar{\mathfrak{p}}$，故 $\bar{\alpha}_1=(\alpha_0-\delta_0)\xi^{-1}\in\bar{\mathfrak{o}}$，如此重复推理就得 $\delta_1\in\Delta$ 使得 $\bar{\alpha}_1-\delta_1\in\bar{\mathfrak{p}}$ 和 $\bar{\alpha}_2=(\bar{\alpha}_1-\delta_1)\xi^{-1}\in\bar{\mathfrak{o}}$．得 $\bar{\alpha}=\delta_0+\delta_1\xi+\bar{\alpha}_2\xi^2$，$\bar{\alpha}_2\in\bar{\mathfrak{o}}$．如同 p-adic 数一样，可继续此过程并得到

$$\bar{\alpha}=\delta_0+\delta_1\xi+\delta_2\xi^2+\cdots+\delta_k\xi^k+\bar{\alpha}_{k+1}\xi^{k+1},\tag{22}$$

其中 $\delta_i\in\Delta$，$\bar{\alpha}_{k+1}\in\bar{\mathfrak{o}}$．由于 $\nu(\bar{\alpha}_{k+1}\xi^{k+1})\geqslant k+1$，显然序列 $\{\bar{\alpha}_k\xi^k\}$ 是零序列．故有

$$\bar{\alpha}=\delta_0+\delta_1\xi+\delta_2\xi^2+\cdots,\delta_i\in\Delta,\tag{23}$$

对任意 $\bar{\alpha}\in\bar{\mathfrak{o}}$．如果 $\bar{\beta}$ 是 $\bar{\Phi}$ 的任一元，可记 $\bar{\beta}=\bar{\alpha}\xi^{-k}$，其中 k 是非负整数，$\bar{\alpha}\in\bar{\mathfrak{o}}$．则有

$$\bar{\beta}=\xi^{-k}(\delta_0+\delta_1\xi+\delta_2\xi^2+\cdots).\tag{24}$$

这表明 $\bar{\Phi}$ 是形如(24)的关于 ξ 的系数在域 Δ 中的幂级数集．易知表示式(24)对 $\bar{\beta}$ 是唯一的，就是说，k 和 $\delta_i\in\Delta$ 是被 $\bar{\beta}$ 唯一确定的．$\bar{\Phi}$ 中元的加法和乘法按通常的形式幂级数运算，而后者则基于 Δ 中的运算．例如，$(\delta_0+\delta_1\xi+\cdots)+(\varepsilon_0+\varepsilon_1\xi+\cdots)=(\delta_0+\varepsilon_0)+(\delta_1+\varepsilon_1)\xi+\cdots$，对 δ_i，$\varepsilon_i\in\Delta$；又 $\left(\sum_0^\infty\delta_i\xi^i\right)$

$\left(\sum_0^{\infty} \varepsilon_j \xi^j\right) = \sum_0^{\infty} \eta_k \xi^k$，其中 $\eta_k = \sum_{i=0}^{k} \delta_i \varepsilon_{k-i}$. 显然，我们已经可以象对形式幂级数(24)的域那样很好地把握了域 Φ.

其次我们考虑Δ是特征 $p \neq 0$ 的完全域，并从此出发构造域 Φ，使 Φ 为 p-adic 数域的推广，我们将给出的构造是基于已在§3.4 中考虑过的维特向量. 我们从基于 I_p 上的一个交换代数 $\mathfrak{U}$ 的维特向量(无限长的)环 $\mathfrak{W}(\mathfrak{U})$ 的定义开始. $\mathfrak{W}(\mathfrak{U})$ 的元是无限序列

(25) $$(a_0, a_1, a_2, \cdots), \quad a_i \in \mathfrak{U},$$

这里相等被定义为对应分量相等，我们用第三章公式(22)定义加法和乘法，这些公式曾被用来确定 $\mathfrak{W}_m(\mathfrak{U})$ 的合成，$\mathfrak{W}_m(\mathfrak{U})$ 是定义在 $\mathfrak{U}$ 上的长为m的维特向量的环. 然后我们能证明 $\mathfrak{W}(\mathfrak{U})$ 是一个环. 但是，更方便的是用一个等价的但稍有不同的方法，此方法是环的逆向极限的一种特殊情形. 在当前的情况下，我们处理环 $\mathfrak{U} = \mathfrak{W}_1(\mathfrak{U}), \mathfrak{W}_2(\mathfrak{U}), \cdots$的这样的极限，在 $\mathfrak{W}_m(\mathfrak{U})$ 到 $\mathfrak{W}_{m-1}(\mathfrak{U})$ 内存在限制同态 R. 与 $\mathfrak{W}(\mathfrak{U})$ 的元 $A = (a_0, a_1, \cdots)$ 对应的是它在 $\mathfrak{W}_m(\mathfrak{U})$ 中的射影 $A^{\pi_m} = (a_0, a_1, \cdots, a_{m-1})$. 则 $A^{\pi_m R} = (a_0, \cdots, a_{m-2}) = A^{\pi_{m-1}}$. 另一方面，$\{A_m | m = 0,1,2,\cdots\}$ 是元 $A_m \in \mathfrak{W}_m(\mathfrak{U})$ 的任一序列且 $A_m^R = A_{m-1}$, $m = 1,2,\cdots$，则显然存在唯一的 $A \in \mathfrak{W}(\mathfrak{U})$，使 $\{A_m\} = A^{\pi_m}$. 因此，我们可以把$\mathfrak{W}(\mathfrak{U})$的元同序列 $\{A_m\}$ 等同起来，这里 $A_m \in \mathfrak{W}_m(\mathfrak{U})$，且 $A_m^R = A_{m-1}$. 如果 $A = \{A_m\}$ 和 $B = \{B_m\}$ 是两个这样的序列，我们定义 $A + B = \{A_m + B_m\}$, $AB = \{A_m B_m\}$. 由于R为环同态，则 $(A_m + B_m)^R = A_m^R + B_m^R = A_{m-1} + B_{m-1}$, $(A_m B_m)^R = A_m^R B_m^R = A_{m-1} B_{m-1}$. 故 $A + B, AB \in \mathfrak{W}(\mathfrak{U})$. 容易验证 $\mathfrak{W}(\mathfrak{U})$ 关于这些结合法是一个交换环且 $0 = (0,0,0\cdots)$, $1 = (1,0,0,\cdots)$. 对固定的 m，映射 $\pi_m: A \to A^{\pi_m}$ 是$\mathfrak{W}(\mathfrak{U})$ 到 $\mathfrak{W}_m(\mathfrak{U})$ 上的一个同态，由于1^{π_m}的阶为 p^m，显然 $\mathfrak{W}(\mathfrak{U})$ 的单位元 1 在加法群$(\mathfrak{W}(\mathfrak{U}), +)$中的阶为无限.

设 $\mathfrak{N}_m$ 表示 π_m 的核，则 $\mathfrak{N}_m$ 是 $\mathfrak{W}(\mathfrak{U})$ 中形如 $(0, \cdots, 0,$

$a_m, a_{m+1}, \cdots$)的元的集，因此

$$(26) \qquad \mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \mathfrak{N}_3 \supset \cdots, \bigcap_{m=1}^{\infty} \mathfrak{N}_m = 0.$$

我们能利用集 $\{\mathfrak{N}_m\}$ 去定义 $\mathfrak{W}(\mathfrak{A})$ 中的收敛性：若 $\{A_k | k = 1, 2, \cdots\}$ 是 $\mathfrak{W}(\mathfrak{A})$ 中元的一个序列，如果对任一个正整数 m 存在一个正整数 $N(m)$ 使对一切 $k \geqslant N(m)$ 有 $A - A_k \in \mathfrak{N}_{N(m)}$，则我们称 $\{A_k\}$ 收敛于 $\mathfrak{W}(\mathfrak{A})$ 的元 $A(A_k \to A)$。易知极限 A 是唯一的且由 $A_k \to A, B_k \to B$ 得 $A_k \pm B_k \to A \pm B, A_k B_k \to AB$。设 $\{C_k | k = 0, 1, 2, \cdots\}$ 是一个序列，而 $C_k \in \mathfrak{N}_k$，$k = 1, 2, \cdots$，令 $A_k = C_0 + C_1 + \cdots + C_k$，则 $A_m^{\pi_{m+1}R} = A_m^{\pi_m} = A_{m-1}^{\pi_m}$；因此元 $A_m^{\pi_{m+1}} \in \mathfrak{W}_{m+1}(\mathfrak{A})$ 的序列 $\{A_m^{\pi_{m+1}}, m = 0, 1, 2 \cdots\}$ 能与元 $A \in \mathfrak{W}(\mathfrak{A})$ 等同起来。我们验证 $A_k \to A$：因为 $A_k = C_0 + C_1 + \cdots + C_k$，我们将用记号 $\sum_{k=0}^{\infty} C_k = A$ 表示 A_k 收敛于 $A(A_k \to A)$。

我们知道，如果 $\mathfrak{N}$ 是 $\mathfrak{W}_m(\mathfrak{A})$ 中元 $(0, a_1, \cdots, a_{m-1})$ 的理想，则 $\mathfrak{N}$ 是幂零的(定理 3.12)。事实上，此结果的证明表明 $\mathfrak{N}^k$ 包含在形如 $(0, \cdots, 0, a_{k-1}, \cdots, a_{m-1})$ 的向量集里，由此在 $\mathfrak{W}(\mathfrak{A})$ 中得 $\mathfrak{N}_1^k \subseteq \mathfrak{N}_k$。因此，如果 $Z \in \mathfrak{N}_1$，则 $\sum_{k=0}^{\infty} Z^k$ 是确定的。由于 $\left(\sum_0^m Z^k\right)(1 - Z) = 1 - Z^{m+1}$，于是 $1 - Z$ 是 $\mathfrak{W}(\mathfrak{A})$ 中的单位，以 $\sum_0^{\infty} Z^k$ 作为逆元。由 $(a_0, \cdots)(a_0^{-1}, \cdots) = (1, \cdots)$ 得到，如果 a_0 是 $\mathfrak{A}$ 中的单位，则 $(a_0, a_1, \cdots)$ 是 $\mathfrak{W}(\mathfrak{A})$ 中的单位。

现设 $\mathfrak{A} = \Delta$ 是特征 p 的完全域，则由 §3.4(等式(27))建立的 $\mathfrak{W}_m(\mathfrak{A})$ 中的公式 $p(a_0, a_1, \cdots, a_{m-1}) = (0, a_0^p, a_1^p, \cdots, a_{m-2}^p)$ 推出 $p(a_0, a_1, \cdots) = (0, a_0^p, a_1^p, \cdots)$ 在 $\mathfrak{W}(\mathfrak{A})$ 中成立，反复应用这一公式得出

$$(27) \qquad p^k(a_0, a_1, \cdots) = (\overbrace{0, \cdots, 0}^{k}, a_0^{p^k}, a_1^{p^k}, \cdots).$$

由于 $\mathfrak{U}=\Delta$ 是完全的，元 $a_i^{p^k}$ 能取成Δ中的任一元，因此我们有 $p^k\mathfrak{W}(\Delta)=\mathfrak{N}_k$，而 $\mathfrak{N}_k$ 是我们在前面定义过的理想．(27) 还表明，如果 $A\neq 0$，则对 $k=1,2,\cdots$ 有 $p^kA\neq 0$．现令A和B是 $\mathfrak{W}(\Delta)$ 中任意非零的元，则可以记 $A=p^kC, B=p^lD$，这里 $C, D\in\mathfrak{N}_1$．那么 $C=(c_0,\cdots)$ 和 $D=(d_0,\cdots)$，这里 $c_0\neq 0$，$d_0\neq 0$．因此 $CD=(c_0d_0,\cdots)\neq 0$ 和 $AB=p^{k+l}CD\neq 0$．这表明 $\mathfrak{W}(\Delta)$ 是个整区．设Φ是 $\mathfrak{W}(\Delta)$ 的分式域，并考虑Φ中形如 p^kC 的元所成的子集 Φ'，其中 $C\in\mathfrak{W}(\Delta)$，$k=0,\pm 1,\pm 2,\cdots$．由于任何 $C\in\mathfrak{W}(\Delta)$，$\notin p\mathfrak{W}(\Delta)$[1]是 $\mathfrak{W}(\Delta)$ 中的单位，显然 Φ' 中的非零元关于乘法成为一个群．因为 Φ' 是Φ的包含 $\mathfrak{W}(\Delta)$ 的子环，故 $\Phi'=\Phi$.

如果 $A=p^kC$，$C\in\mathfrak{W}(\Delta)$，$\in\mathfrak{N}_1$，则我们定义序函数 $\nu(A)=k$，并定义 $\varphi(A)=p^{-k}$，$\varphi(0)=0$．那么φ是Φ的非阿基米得赋值．子环 $\mathfrak{W}(\Delta)$ 是满足 $\varphi(A)\leqslant 1$ 的元的集，而 $\mathfrak{N}_1$ 是 $\mathfrak{W}(\Delta)$ 中满足 $\varphi(B)<1$ 的元B的理想．剩余环为 $\mathfrak{W}(\Delta)/\mathfrak{N}_1$ 且同构于 Δ．由前面我们关于 $\mathfrak{W}(\mathfrak{U})$ 中序列收敛性的结果可得到Φ关于赋值φ是完备的．此结果留给读者验证． 由于1是无限阶的，则Φ的特征为0．这样Φ有我们所要求的一切性质：关于一个非阿基米得实赋值是完备的，特征为0，以给定的特征为p的完全域Δ为剩余域．如果从 $\Delta=I_p$ 出发，则我们用此方法得到的域Φ是 p-adic 数域．

8. 有序群和赋值 一个非阿基米得实赋值满足 $\varphi(\alpha+\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta))$，$\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)$．因此，在考虑这样一个赋值的时候，实数的加法显然不起作用，只有乘法和非负实数的序包含在定义的性质中．如我们将看到的，这就导致将非阿基米得实赋值概念推广为值在任一有序交换群中的(非阿基米得)赋值．此推广除了增加结果的普遍性外，重要的是较原来的概念更简单和更自然．我们首先考虑有序交换群的概念．

---

1) 原文误为 $\mathfrak{W}(A)$——译者注．

定义 6. 有序(交换)群 G 为交换群 G 连同满足如下三条件的子集 H:1)$1 \notin H$,2)如果 $a \in G$,那么或者 $a \in H$,或者 $a = 1$,或者,$a^{-1} \in H$,3)H 关于 G 的乘法是封闭的.

如果 (G,H)是一个有序群,那么我们令 $H^{-1} = \{b^{-1} | b \in H\}$,则条件 2 表明 $G = H \cup \{1\} \cup H^{-1}$,而且这些子集互不重迭.对 H 和 $\{1\}$ 这是条件 1 的假设;对 H^{-1} 和 $\{1\}$,若 $1 \in H^{-1}$,则 $1 \in H$,这与条件 1 矛盾,故 H^{-1} 和 $\{1\}$ 不重迭;最后,如果 $a \in H \cap H^{-1}$,则 $a^{-1} \in H$ 并由条件 3 得 $1 = aa^{-1} \in H$,这与条件 1 矛盾.

正实数形成一个有序群,如果取 H 为 < 1 的正实数集. 取 H 为 > 1 的正实数集同样也是可以的. 事实上,若 G 为任一有序群,则 H^{-1} 对 G 的乘法是封闭的并满足定义 6 的条件 1 和 2,那么我们用 H^{-1} 代替 H 就得到另一个有序群. 在任一个有序群 G 中如果 $ab^{-1} \in H$,我们定义: $a < b$. 这就在 G 中确定了一个线性序,就是说,我们有下述性质: 1.如果 $a < b, b < c$,则 $a < c$.2.对任一对 (a,b),$a,b \in G$,有且仅有一种下述关系成立: $a < b$, $a = b$, $b < a$ (我们经常把 $a < b$ 记为 $b > a$). G 中的序对乘法保持不变,就是说,有: 3. 如果 $a < b$,则 $ac < bc$. 反之,如果在群 G 中定义了一种关系 $a < b$ 并满足性质 1,2 和 3,则 G 对于子集 $H = \{a | a < 1\}$ 是有序的. 显然,定义 6 的条件 1 对 H 成立. 往证条件 2 和条件 3: 首先,我们注意到,如果 $a < b$ 和 $c < d$ 则 $ac < bc < bd$,那么 $ac < bd$; 因此,$a < b$ 当且仅当 $a^{-1} > b^{-1}$. 特别地,$a < 1$ 当且仅当 $a^{-1} > 1$. 因为任一个 a 满足条件之一: $a < 1$, $a = 1$, $a > 1$,故显然满足定义 6 的条件 2. 最后,由 $a < 1, b < 1$ 得到 $ab < 1$,于是 H 对 G 的乘法是封闭的. 我们还指出由 H 按下述方法: 若 $ab^{-1} \in H$,则 $a < b$,定义的序与原来的序相同,因为 $ab^{-1} \in H$ 意味着 $ab^{-1} < 1$ 这当且仅当 $a < b$ 时成立.

如果 G_1 是有序群 G 的一个子群,而 G 由集 $H = \{a | a \in G, a > 1\}$ 序化,则 G_1 有一个由 $H_1 = G_1 \cap H$ 定义的导出序. 这可以直接证明,或者也可以由下述说明看出: G 中的关系 $>$ 可给

出 G_1 的一个关系，它满足前述的条件. 如果G被H序化，G'是第二个有序群，被 H' 序化，则G到 G' 内的一个使 $H\eta\subseteq H'$ 的同构 η 称为序同构. 如果存在一个G到 G' 上的序同构 η，则称G和 G' 是序同构的. 此时必有 $H\eta = H'$. 例如，正实数关于乘法的群，而H如前所定义的，是序同构于一切实数关于加法的群，此群被负实数集 H' 序化. 映射 $a\to\log a$ (自然对数)是第一个群到第二个群上的序同构.

如果G是一个有序群，则G不包含有限阶的 $\neq 1$的元. 因为，如果 $a<1(a>1)$，则 $a^n<1(a^n>1)$，那么对每个正整数n，$a^n\neq 1$. G的此性质的一个结果是，对任意固定的整数 n，G 的映射 $x\to x^n$是G到G的一个子群上的同构；若 $n\geqslant 1$，则此映射是保序的.

为了定义一般赋值，我们需要考虑具有0的有序群 V. 要定义这样一个体系，它是一个有序群G和添加一个元0组成: $V=G\cup\{0\}$. 对每个 $a\in G$ 定义 $0<a$，并对一切a定义 $a0=0$，就可把G的序扩充至 V. 于是给出下列的

定义 7. 设Φ是一个域，V是一个具有0的有序(交换)群，称Φ到V内的映射 $\varphi:\alpha\to\varphi(\alpha)$ 为赋值，如果

(i) $\varphi(\alpha)=0$ 当且仅当 $\alpha=0$.

(ii) $\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)$.

(iii) $\varphi(\alpha+\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta))$.

不久就会清楚此定义的精确范围. 此刻，若在定义中把V取为非负实数，则易知实非阿基米得赋值是一种特殊情形；另一方面，需要指出的是：实阿基米得赋值不是这个意义下的赋值. 这术语的不一致不会引起什么实质性的麻烦. 现在给出一个赋值的例子，其V不是非负实数.

例 在本例中我们将发现对群G 使用加法记号是方便的. 在定义7中由这一变化引起的必要修改是明显的，故我们毋需重述. 我们考虑的群G是整数对 (k,l) 的加群，在G中引进字典序，即若 $k<k'$ 时或 $k=k'$ 而 $l<l'$ 时，定义 $(k,l)<(k',l')$. 可验证这是一个对加法保持的线性序；故 G是一个有序(加法)群. 设 $V=G\cup\{\infty\}$，若对每个 $(k,l)\in G$，令$\infty>(k,l)$，就把G的序扩充到 V. 还定义 $(k,l)+\infty=\infty$.

令 $P=\Phi(\xi,\eta)$ 是域Φ的一个纯超越扩张，这里的 $\{\xi,\eta\}$ 是P在Φ上的一个超越基．若 $a\in P$ 且 $a\neq 0$，可记 $a=\xi^m\eta^n p(\xi,\eta)q(\xi,\eta)^{-1}$，其中 $p(\xi,\eta)$ 和 $q(\xi,\eta)$ 是ξ,η 的常数项非零的多项式，而m和n为整数．我们定义 $\varphi(a)=(m,n)$，且令$\varphi(0)=\infty$．则(i)保持，容易验证 $\varphi(ab)=\varphi(a)+\varphi(b)$ 和 $\varphi(a+b)\geqslant\min(\varphi(a),\varphi(b))$．能否对加法记号就是(ii)，若颠倒此序(把＜改为＞)后若就可变成(iii)．故我们的函数确实是一个赋值．

习　题　39

1．设G是上例中整数对 (k,l) 的加法有序群，c和e为实数满足$0<c<1$且e为正无理数．证明映射 $(k,l)\to c^{k+el}$是G到正实数的有序乘法群P内的一个同构．证明G不能序同构于P的子群．

2．设 $P=\Phi(\xi,\eta)$，$a=\xi^m\eta^n p(\xi,\eta)q(\xi,\eta)^{-1}$，其中$p$和$q$同上例，是$\xi,\eta$ 的常数项不为零的多项式．定义 $\phi(a)=c^{m+en}$，其中c和e为实数，$0<c<1$，e为正无理数．证明ϕ是一个非阿基米得实赋值，但不是离散的．

3．在定义7中用整区$\mathfrak{o}$代替域Φ并定义整区$\mathfrak{o}$的赋值 φ．证明$\mathfrak{o}$到V内的任一赋值ϕ可唯一地扩充为$\mathfrak{o}$的分式域Φ的赋值．

4．设G为任意的(交换)有序群，$\mathfrak{o}=\Phi_0(G)$ 是G的在域 Φ_0 上的群环(卷1，习题39的第2题，中译本 p.89)，证明 $\mathfrak{o}$是一个整区．若 $a=\sum_1^r \alpha_i g_i$，$\alpha_i(\neq 0)\in\Phi_0$，$g_i\in G$，定义 $\varphi(a)=\min g_i$ (对于G所定义的序＜来说)，规定 $\varphi(0)=0$，证明φ是$\mathfrak{o}$的一个赋值，利用第3题和第4题证明：若V是任一个具有0的有序群，则存在一个域 Φ，它具有Φ到V内的一个赋值φ使得 $\varphi(\Phi)=V$．

9. 赋值，赋值环与位　在这一节，将在定义7意义下的赋值概念和另外两个概念之间建立等价性，此两个概念是赋值环和位．赋值环是一个内在的概念，即是说它的定义不需要任何外加于给定的域Φ上的体系．再者，赋值环给出了赋值和位之间的联系．对实非阿基米得赋值，我们已经见过这些概念．

现设Φ是任意域，而φ是值在有序群V (具有0)内的一个赋值．首先注意到 $\varphi^2(1)=\varphi(1^2)=\varphi(1)$，而且由于$G$不包含有限阶元$\neq 1$，故 $\varphi(1)=1$．又因 $\varphi(-1)^2=\varphi(1)=1$，故 $\varphi(-1)=1$，$\varphi(-\alpha)=\varphi(-1)\varphi(\alpha)=\varphi(\alpha)$．从 $\alpha\alpha^{-1}=1$ 得到$\varphi(\alpha^{-1})=\varphi(\alpha)^{-1}$ 和 $\varphi(\alpha\beta^{-1})=\varphi(\alpha)\varphi(\beta)^{-1}$．现设 $\mathfrak{o}$ 是Φ中使 $\varphi(\alpha)\leqslant 1$ 的元α形成的子集．若$\alpha,\beta\in\mathfrak{o}$，则 $\varphi(\alpha-\beta)\leqslant\max(\varphi(\alpha),\varphi(\beta))\leqslant 1$，$\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)\leqslant 1$．因此 $\mathfrak{o}$ 是一个子环．设α

$\notin \mathfrak{o}$,则 $\varphi(\alpha)>1$ 且 $\varphi(\alpha^{-1})=\varphi(\alpha)^{-1}<1$. 故 $\alpha^{-1}\in\mathfrak{o}$. 因此，$\mathfrak{o}$ 在下述的意义上是一个赋值环(在 Φ 内):

定义 8. 若 Φ 是一个域，Φ 中的一个赋值环 $\mathfrak{o}$ 是 Φ（包含 1）的一个子环，使得 Φ 的每个元或者属于 $\mathfrak{o}$ 或者是 $\mathfrak{o}$ 的一个元的逆元.

若对于赋值 φ,$\mathfrak{o}$ 是满足 $\varphi(\alpha)\leqslant 1$ 的元 α 的子环，则称 $\mathfrak{o}$ 为 φ 的赋值环. 这是我们在前面给出的定义的一个对非阿基米得实赋值之直接推广，我们现在证明：任一赋值环引出一个赋值 φ'，使给定的环是 φ' 的赋值环. 设 $\mathfrak{o}$ 是 Φ 的一个赋值环，U 是 $\mathfrak{o}$ 的单位的集，$\mathfrak{p}$ 是非单位的集，$\mathfrak{p}^*$ 为不等于零的非单位的集，Φ^* 是 Φ 的非零元的乘法群，则 U 是交换群 Φ^* 的一个子群，我们取 $G'=\Phi^*/U$. 设 H' 是陪集 βU，$\beta\in\mathfrak{p}^*$，所组成的集，我们在 G' 中引进一个序. 显然 $\mathfrak{o}$ 的一个非单位与 $\mathfrak{o}$ 的一元的积是非单位，因此，若 $\beta_1,\beta_2\in\mathfrak{p}^*$，则 $\beta_1\beta_2\in\mathfrak{p}^*$；那么，若 $\beta_1U,\beta_2U\in H'$，则 $(\beta_1U)(\beta_2U)=\beta_1\beta_2U\in H'$. 若 βU 为 $G'=\Phi^*/U$ 的任一元，则 $\beta\neq 0$，且若 $\beta\notin\mathfrak{p}^*$，则 $\beta\in U$ 或者 $\beta\notin U$ 且 $\beta\notin\mathfrak{p}^*$. 在第一种情形 $\beta U=U$，在第二种情形 $\beta\notin\mathfrak{o}$，那么 $\beta^{-1}\in\mathfrak{o}$，而且由于 $\beta^{-1}\in U$ 推得 $\beta\in U$，我们有 $\beta^{-1}\in\mathfrak{p}^*$. 因此 $(\beta U)^{-1}=\beta^{-1}U\in H'$. 故 $G'=H'\cup\{1\}\cup(H')^{-1}$ 成立. 又 $1=U\notin H'$. 所以 H' 使 G' 在定义 6 的意义下成为一个有序群. 其次，添加 0 到 G' 得 $V'=G'\cup\{0\}$，并利用

(28) $\qquad \varphi'(0)=0$，$\varphi'(\alpha)=\alpha U\in G'$，若 $\alpha\neq 0$，定义 Φ 到 V' 内的一个映射 φ'. 它显然满足赋值的条件 (i)和 (ii). 若 $\alpha=0$ 或 $\beta=0$ 满足条件(iii)也是显然的. 如果 $\alpha\neq 0$，$\beta\neq 0$，则 $\alpha\beta^{-1}\in\mathfrak{o}$ 或者 $\beta\alpha^{-1}\in\mathfrak{o}$，我们不妨设为前者，则得 $\alpha=\beta\gamma$，其中 $\gamma\in\mathfrak{o}$，并且由于 $\varphi'(\gamma)=\gamma U\leqslant 1=U$，得 $\varphi'(\alpha)=\varphi'(\beta)\varphi'(\gamma)\leqslant\varphi'(\beta)$. 又由于 $\alpha\beta^{-1}+1\in\mathfrak{o}$，于是 $\varphi'(\alpha\beta^{-1}+1)\leqslant 1$ 和 $\varphi'(\alpha+\beta)=\varphi'(\alpha\beta^{-1}+1)\varphi'(\beta)\leqslant\varphi'(\beta)=\max(\varphi'(\alpha),\varphi'(\beta))$. 故 (iii) 成立. 由(28) 和 G' 及 H' 的定义易知 $\varphi'(\alpha)\leqslant 1$ 等价于 $\alpha\in\mathfrak{o}$. 因此 $\mathfrak{o}$ 是赋值 φ' 的赋值环. 我们称此赋值 φ' 为赋值环 $\mathfrak{o}$

的典范赋值.

现在再考虑Φ到 $V=(G,0)$ 内的任一赋值 φ，而G为H序化的交换群，设 $\mathfrak{o}$ 是φ的赋值环，而 φ' 为Φ到 $V'=(G',0)$ 内的典范赋值，这里 $G'=\Phi^*/U$ 被 $H'=\{\beta U|\beta\in\mathfrak{p}^*\}$ 所序化.定义(28)给出 $\varphi'(0)=0$，若 $\alpha\neq 0$，则 $\varphi'(\alpha)=\alpha U$. 我们得到乘群$\Phi^*$到$G$内的同态$\alpha\to\varphi(\alpha)$，其核为子群$U$. 因此，我们有 $G'=\Phi^*/U$ 到G内的诱导同构 $\eta:\varphi'(\alpha)=\alpha U\to\varphi(\alpha)$. 由于从 $\beta U\in H'$ 可得 $\beta\in\mathfrak{p}^*$，于是 $\varphi(\beta)<1$，故这是一个序同构. 我们看到给定的赋值可分解成 $\varphi=\varphi'\eta$，其中η是 G' 到G 内的一个序同构(严格说来是 V' 到V内的).

这些想法自然把具有相同赋值环 $\mathfrak{o}$ 的Φ的赋值的概念统一起来了. 据此，将称这样的赋值是等价的.

第三个概念是位，它也等价于赋值和赋值环的概念. 定义如下:

定义 9. 若Φ是一个域，位$\mathscr{P}$是Φ的一个子环 $\mathfrak{o}$ 到一个域Δ内的同态，使得如果 $\alpha\notin\mathfrak{o}$，则 $\alpha^{-1}\in\mathfrak{o}$ 且 $\mathscr{P}(\alpha^{-1})=0$. (注意，我们对子环和同态约定有 $1\in\mathfrak{o}$ 且 $\mathscr{P}(1)=1$.)

由此定义显然有：若$\mathscr{P}$是一个位，则由$\mathscr{P}$给出的子环 $\mathfrak{o}$ 是一个赋值环. 另一方面，假设 $\mathfrak{o}$ 是任一赋值环，$\mathfrak{p}$ 是 $\mathfrak{o}$ 的非单位的集. 那么，显然有：如果 $\beta\in\mathfrak{p}$ 且 $\alpha\in\mathfrak{o}$ 则 $\alpha\beta\in\mathfrak{p}$. 特别，$-\beta=(-1)\beta\in\mathfrak{p}$. 如果 β_1 及 $\beta_2\in\mathfrak{p}$，我们可设 $\beta_1\beta_2^{-1}\in\mathfrak{o}$，则 $\beta_1\beta_2^{-1}+1\in\mathfrak{o}$，那么 $\beta_1+\beta_2=(\beta_1\beta_2^{-1}+1)\beta_2\in\mathfrak{p}$. 因此，$\mathfrak{p}$ 是 $\mathfrak{o}$ 的一个理想. 由于 $\mathfrak{p}$ 是 $\mathfrak{o}$ 的非单位的集，故 $\mathfrak{p}$ 是极大的且 $\Delta'=\mathfrak{o}/\mathfrak{p}$ 是一个域. 设 $\mathscr{P}'$ 是由 $\mathfrak{o}$ 到 $\Delta'=\mathfrak{o}/\mathfrak{p}$ 上的典范同态，则$\mathscr{P}$和 $\mathfrak{o}$ 显然满足位的定义中要求的条件. 我们将称这个位为赋值环 $\mathfrak{o}$ 的典范位. 在 $\mathscr{P}'$ 下 $\mathfrak{o}$ 的象是 $\Delta'=\mathfrak{o}/\mathfrak{p}$，其中 $\mathfrak{p}$ 是 $\mathfrak{o}$ 中非单位的理想.与实非阿基米得赋值的特殊情况一样，将把 Δ' 称为赋值环 $\mathfrak{o}$ 的剩余域.

现仍考虑Φ到域Δ内的任一个位$\mathscr{P}$，设 $\mathfrak{o}$ 为赋值环，$\mathscr{P}$定义于其上.设 $\mathfrak{p}$ 是 $\mathfrak{o}$ 中非单位的理想.如果 $\alpha\in\mathfrak{p}$ 且 $\alpha\neq 0$，则 α^{-1}

$\notin \mathfrak{o}$，那么由对$\mathscr{P}$的假设得到$\mathscr{P}(\alpha)=0$。若 $\alpha=0$ 此式也成立。因此，$\mathfrak{p}$ 含于$\mathscr{P}$的核中。由于 $\mathfrak{p}$ 是一个极大理想，这表明 $\mathfrak{p}$ 就是$\mathscr{P}$的核。所以，由同态 $\alpha\to\mathscr{P}(\alpha)(\alpha\in\mathfrak{o})$ 得出同构 $\mathscr{P}'(\alpha)=\alpha+\mathfrak{p}\to\mathscr{P}(\alpha)$，那么位$\mathscr{P}$是典范位$\mathscr{P}'$和 Δ'到Δ内一个同构的结式。至于赋值，自然可作为有相同赋值环的等价位来考虑。

于是，我们建立了从赋值、赋值环、位三个概念中的一个转化到其余两个的步骤。显然，关于这些概念中某一个的结论可以变成另外两个的相应的结论。以后，我们将应用这一思想由位的扩张得到赋值的扩张。后者归结到同态的扩张，对此可利用导言中的基本扩张定理。

习　题　40

1. 设$\mathscr{P}$是Φ上其值在Δ内的一个位。添加一个新元∞到Δ并定义 $\infty+\delta=\infty=\delta+\infty$，$\delta\in\Delta$，$\infty\infty=\infty$，$\infty\delta=\infty=\delta\infty$，这里 $\delta\in\Delta$，$\delta\neq0$。若 $\alpha\notin\mathfrak{o}$，定义 $\mathscr{P}(\alpha)=\infty$，扩张$\mathscr{P}$到整个 Φ。证明

$$\mathscr{P}(\alpha+\beta)=\mathscr{P}(\alpha)+\mathscr{P}(\beta),\qquad (29)$$

$$\mathscr{P}(\alpha\beta)=\mathscr{P}(\alpha)\mathscr{P}(\beta),$$

当右边被确定以后。反之，设$\mathscr{P}$是一个定义在Φ上的函数，它的值在(Δ,∞)中，Δ为域而$\Delta\cap\{\infty\}=\varnothing$，且$\infty$遵从所指出的规划。当(29)的右边是确定的时候，假定(29)成立。设$\mathfrak{o}$ 是逆象 $\mathscr{P}^{-1}(\Delta)$。证明$\mathscr{P}$到 $\mathfrak{o}$ 的限制是一个位。这就给出了位的另一个定义。

2. 设$\mathscr{P}$是一个具有赋值环 $\mathfrak{o}$的位，$\mathscr{P}$是一个同构。证明 $\mathfrak{o}=\Phi$ 而且 $\mathfrak{o}$的典范赋值是平凡的，即 $\varphi'(0)=0$，如果 $\alpha\neq0$，$\varphi'(\alpha)=1$。

10. 实非阿基米得赋值的刻划　为了把赋值的一般理论应用到非阿基米得实赋值的情形，我们需要刻划一个域的所有可能的赋值。按前面讨论的观点，这等价于刻划有序群的问题，而此有序群是序同构于正实数乘法群之子群，或者等价地，是序同构于(关于通常的序）所有实数加法群之子群。因此我们要找出序同构于实数加群之子群的有序群的刻划。本节中我们所考虑的一切群使用加号将更为方便。

设G是一个有序群：如果 $a\in G$，我们规定：当 $a\geq0$ 时，$|a|=a$；当 $a<0$ 时，$|a|=-a$。我们定义G的一个孤立子群

K,它是一个子群满足：若 $a\in K$ 且 $|b|\leqslant|a|$，则 $b\in K$. 设 K_1 和 K_2 是孤立子群，那么我们断言 $K_1\subseteq K_2$ 或者 $K_2\subseteq K_1$. 因为，如果这些包含关系均不成立，则存在一个 $b_1\in K_1, b_1\notin K_2$，且存在一个 $b_2\in K_2, b_2\notin K_1$，并可设 $b_i>0$. 如果 $b_2>b_1$，则 $b_1\in K_2$，这与假定矛盾. 因此，$b_2\ngtr b_1$，同理 $b_1\ngtr b_2$，但这与 G 是一个有序群矛盾. 因此有 $K_1\supseteq K_2$，或者 $K_2\supseteq K_1$，那么孤立子群的集对于包含关系有线性序. 孤立子群集的序型称为 G 的**秩**[1]. 最简单的情形是**秩1**的群，这样的群 $G\neq 0$ 且 G 没有 $\neq 0$，G 的孤立子群. 这些群可以用阿基米得性质来刻划，这在实数中是我们所熟知的：

引理. 一个有序群 $G(\neq 0)$ 是秩 1 的当且仅当任意给定 $a,b\in G, a>0$，存在正整数 n 使得 $na>b$.

证. 首先设 G 含有两个元 a,b，使得 $a>0$ 且对一切正整数 n 有 $na\leqslant b$. 令 K_+ 记 G 的元 u 的子集，使得对某个正整数 m 有 $0<u<ma$. 由于 $a<2a$，K_+ 非空且显然 K_+ 对加法封闭，并且，K_+ 包含每个 v，使得对某个 $u\in K_+$，$0<v<u$. 因此，如果 u_1 和 $u_2\in K_+$ 且 $u_1<u_2$，则 $0<u_2-u_1<u_2$，那么 $u_2-u_1\in K_+$. 由此得 K_+，0 和 $-K_+$ 的并是 G 的一个子群 K，这里 $-K_+$ 是 K_+ 中元的负元的集，于是 K 是孤立的，这是因为如果 $u\in K$ 且 $u>0$，则每个使 $0<v\leqslant u$ 的 v 属于 K. 由于 $b\notin K$ 还有 $K\neq G$. 故 G 不是秩 1 的. 反之，设 G 不是秩 1 的，K 是一个孤立子群 $\neq 0$，G. 由于 $K\neq G$，存在一个正元 b 使对每个 $a\in K$，$b>a$. 在 K 中取 $a>0$，则对所有 $n=1,2,3,\cdots$，$na<b$. 故在 G 中阿基米得性质不真.

由此准则易知，如果 G 是秩 1 的，则 G 的任何非零子群是秩 1 的. 特别是实数加群的任何非零子群是秩 1 的. 而且，由于有下述定理，因此这些群实质上是秩 1 的一切有序群.

定理 8. 任何秩 1 的有序群序同构于实数加群的一个子群.

---

1) 例如参考 F. Hausdorff 的"集论"，第三版，第三章，有中译本，科学出版社，张义良、颜家驹译——著者注.

证　我们将定义一个G到实数加群R内的序同构 η，为此在G中取 $u>0$. 如果 $v>0$,则存在正整数 m,n 的数对 (m,n) 使得 $nv\geqslant mu$. 因此可取 $m=1$ 并由阿基米得性质决定n使得 $nv>u=1u$. 如果 $q\in P$ (正整数集),则 $qnv\geqslant qmu$ 当且仅当 $nv\geqslant mu$. 因此,如果 $r=m/n=m'/n',m,n,m',n'\in P$, 则 $nv\geqslant mu$ 当且仅当 $n'v\geqslant m'u$. 满足此条件的有理数 $r=m/n$ 形成一个集,用 R_v 记之. 如果 $r=m/n$ 且 $s=m'/n'<r,m',n'\in P$,则$m'n<mn'$. 如果 $r\in R_v$, 则 $nv\geqslant mu$ 且$nn'v\geqslant mn'u\geqslant m'nu$. 因此 $n'v>m'u$ 故 $s\in R_v$. 其次我们注意到正有理数集 R_v 是有上界的，否则由刚才证明的结果推出 R_v 是正有理数的完备集,因此,每个正整数k都在 R_v 中,这意味着 $v\geqslant ku,k\in P$. 这就与G的阿基米得性质矛盾. 我们现在定义 v^η 是正实数 $\sup R_v$. 由于对每个 $r\in R_v$, R_v 包含每个 $s\leqslant r$, 显然 R_v 和它的余 R'_v 在正有理数集中决定一个戴得金分割，故 $\sup R_v=\inf R'_v$. 于是令 v_1,v_2 是G的正元且设 $m_1/n_1\in R_{v_1},m_2/n_2\in R_{v_2}$,这里 $m_i,n_i\in P$. 则 $n_1v_1\geqslant m_1u,n_2v_2\geqslant m_2u$ 且 $n_1n_2v_1\geqslant m_1n_2u,n_1n_2v_2\geqslant n_1m_2u$. 故 $n_1n_2(v_1+v_2)\geqslant(m_1n_2+m_2n_1)u$,那么 $m_1/n_1+m_2/n_2\in R_{v_1+v_2}$. 由此得 $(v_1+v_2)^\eta\geqslant v_1^\eta+v_2^\eta$. 另方面，重复刚才所给的论证表明,如果 $m_1/n_1\in R'_{v_1}$ (即,$n_1v_1<m_1u$) 和 $m_2/n_2\in R'_{v_2}$, 则 $m_1/n_1+m_2/n_2\in R'_{v_1+v_2}$. 由于 $v^\eta=\inf R'_v$, 由此得出 $(v_1+v_2)^\eta\leqslant v_1^\eta+v_2^\eta$. 因此

$$(v_1+v_2)^\eta=v_1^\eta+v_2^\eta \tag{30}$$

对G中的正元 v_1,v_2 成立. 定义 $0^\eta=0$ 及 $(-v)^\eta=-v^\eta$,如果 v是正数我们就可以把映射η扩充到整个G. 如果 $v_1\geqslant0,v_2\geqslant0$ 或 $v_1\leqslant0,v_2\leqslant0$ 可直接得到(30)成立. 设 $v_1>0$ 及$v_2<0$, 如果 $v_1+v_2\geqslant0$,记 $v_1=(v_1+v_2)+(-v_2)$,则得$v_1^\eta=(v_1+v_2)^\eta+(-v_2)^\eta=(v_1+v_2)^\eta-v_2^\eta$. 则 $(v_1+v_2)^\eta=v_1^\eta+v_2^\eta$. 如果 $v_1+v_2<0$, 则记 $-v_2=-(v_1+v_2)+v_1$ 则得 $(-v_2)^\eta=(-(v_1+v_2))^\eta+v_1^\eta$. 于是 $-v_2^\eta=-(v_1+v_2)^\eta+v_1^\eta$, (30)也成立. 如果 $v_1<0,v_2>0$ 可类似地证明(30)成立. 故η是G到R内的

一个群同态．如果 $v>0$，则 $v^\eta>0$；因此，无正元属于 η 的核．由此得此核为 0 而 η 是一个同构．由于 η 把正元映入到正元，η 是 G 到 R 内的一个序同构．

关于上述证明有几点是需要注意的：首先，从同构 η 的定义显然有 $u^\eta=1$．其次注意，η 由此性质完全决定，即如果 ζ 是 G 到 R 内的任一序同构，使得 $u^\zeta=1$，则 $\zeta=\eta$．设 $b>0$，并设 m/n 满足 $m/n\geqslant v^\eta$，而 m,n 为正整数，则 $m1\geqslant nv^\eta$ 且 $mu^\eta\geqslant nv^\eta$，$(mu)^\eta\geqslant(nv)^\eta$．因此 $mu\geqslant nv$ 并按这些步骤反推可得 $m/n\geqslant v^\zeta$．类似地，由 $m/n\geqslant v^\zeta$ 可得 $m/n\geqslant v^\eta$．由于这对任何有理数均成立，故得 $v^\eta=v^\zeta$；因此，$\eta=\zeta$．如果 β 是任意正实数，则映射 $x\to\beta x$ 是 R 的一个保序自同构，它映射 $1\to\beta$．由此可得，存在 G 的一个序同构，它把给定的正元 u 映入到 R 内的任意正实数 β．而且，这样一个同构是唯一的．

称一个秩 1 群为**离散的**，如果它同构于整数有序群(正性按通常意义)．在前面我们已注意到(§5)，正实数乘法群的一个子群是离散的当且仅当它含有一个最大元 <1．由此点和定理 8 得到一个秩 1 的有序群是离散的当且仅当它含有一个最小正元．

习　题　41

1．设 $R^{(n)}$ 为实数 ξ_i 的 n 元数组 $x=(\xi_1,\cdots,\xi_n)$ 的加法群．如果第一非零 $\xi_i>0$ 则规定 $x>0$，并用来定义 $R^{(n)}$ 中正元的集．证明此集是一个有序群并决定其孤立子群．

2．如果 n 是 G 的非零孤立子群集的基数，n 是一个正整数，则称有序群 G 为**秩 n 的**．证明任何秩 n 的有序群序同构于第 1 题中群 $R^{(n)}$ 的一个子群．

3．如果秩 n 的有序群 G 的逐次孤立子群的商群均为无限循环群则称 G 为**离散的**，证明任何这样的群是同构于 $R^{(n)}$ 的子群，而 $R^{(n)}$ 为 n 元数组 $a=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 所成的群，而 α_i 为整数．

11．同态与赋值的扩张　在这一节，我们将证明同态扩张的基本定理，而此同态是定义在一个域的子环上的．此结果导致从一个子域到一个域的赋值扩张的一般定理．我们首先证明下述的关键引理．

引理 1． 设 $\mathfrak{o}$ 是域 Φ 的子环，$\mathfrak{m}$ 是 $\mathfrak{o}$ 的一个真理想，如果 a

是Φ的非零元而 $\mathfrak{o}[\alpha]$ 是由 $\mathfrak{o}$ 和α生成的Φ的子环，则由 $\mathfrak{m}$ 在 $\mathfrak{o}[\alpha]$ 中生成的理想 $\mathfrak{m}\mathfrak{o}[\alpha]$ 是 $\mathfrak{o}[\alpha]$ 的真理想，或者 $\mathfrak{m}\mathfrak{o}[\alpha^{-1}]$ 是 $\mathfrak{o}[\alpha^{-1}]$ 的真理想。

证. 若不然：$\mathfrak{m}\mathfrak{o}[\alpha]=\mathfrak{o}[\alpha]$，$\mathfrak{m}\mathfrak{o}[\alpha^{-1}]=\mathfrak{o}[\alpha^{-1}]$，则 $1\in\mathfrak{m}\mathfrak{o}[\alpha]$，$1\in\mathfrak{m}\mathfrak{o}[\alpha^{-1}]$，那么我们有关系式：

(31) $$1=\mu_0\alpha^m+\mu_1\alpha^{m-1}+\cdots+\mu_m,\ \mu_i\in\mathfrak{m},$$

(32) $$1=\nu_0\alpha^{-n}+\nu_1\alpha^{-(n-1)}+\cdots+\nu_n,\nu_j\in\mathfrak{m}.$$

由于 $\mathfrak{m}\neq\mathfrak{o}$，有 $m>0,n>0$ 且可设m和n对关系式(31)和(32)是极小的. 还可设 $m\geqslant n$. 则(32)推出 $\alpha^m=\nu_0\alpha^{m-n}+\nu_1\alpha^{m-n+1}+\cdots+\nu_n\alpha^m$；因此

(33) $$\alpha^m(1-\nu_n)=\nu_0\alpha^{m-n}+\cdots+\nu_{n-1}\alpha^{m-1}.$$

用 $1-\nu_n$ 乘(31)得

(34) $$1-\nu_n=\mu_0(1-\nu_n)\alpha^m+\mu_1(1-\nu_n)\alpha^{m-1}+\cdots+\mu_m(1-\nu_n).$$

因此，由(33)，

$$1-\nu_n=\mu_0(\nu_0\alpha^{m-n}+\cdots+\nu_{n-1}\alpha^{m-1})+\mu_1(1-\nu_n)\alpha^{m-1}+\cdots+\mu_m(1-\nu_n).$$

由于 $\mu_i,\nu_j\in\mathfrak{m}$，用 $m-1$ 代替m就得到形如(31)的另一个关系式，但这与m的极小性矛盾. 证毕.

如果$\mathscr{P}$是一个位，它是域Φ的子环 $\mathfrak{o}$ 到域Δ内的一个同态，则我们将称位$\mathscr{P}$是Δ值的. 我们的主要结果是同态到位的下述扩张定理：

定理 9. 设 $\mathfrak{o}_0$ 是域Φ的一个子环，$\mathscr{P}_0$ 是 $\mathfrak{o}_0$ 到任一个代数闭域 Ω内的一个同态，则 $\mathscr{P}_0$ 能扩张成Φ上的一个Ω值位 $\mathscr{P}$.

证. 我们考虑同态$\mathscr{P}_0$ 的扩张$\mathscr{P}'$ 的集，而$\mathscr{P}'$ 是Φ含 $\mathfrak{o}_0$ 的子环 $\mathfrak{o}'$ 内的同态. 可按通常的方式把这些扩张偏序化：如果$\mathscr{P}''$是$\mathscr{P}'$ 的一个扩张，定义 $\mathscr{P}'<\mathscr{P}''$. 那么，我们照例可应用卓伦引理得到一个极大扩张$\mathscr{P}$，而$\mathscr{P}$是定义在$\Phi$的子环 $\mathfrak{o}$ 上的. 我们证明 $\mathfrak{o}$ 是一个赋值环来完成定理的论证. 于是$\mathscr{P}$关于Φ将是一个Ω值位. 设 $\mathfrak{m}$ 是$\mathscr{P}$的核. 由于 $1\longrightarrow1$，故 $\mathfrak{m}\neq\mathfrak{o}$. 因$\Omega$没

有零因子 $\neq 0$，故 $\mathfrak{m}$ 关于 $\mathfrak{o}$ 是一个素理想．所以，$\mathfrak{m}$ 关于 $\mathfrak{o}$ 的余集M对乘法是封闭的，而且 $0 \in M$．设 $\mathfrak{o}'$ 是Φ中形如 $\alpha\beta^{-1}$ 的元之子集，其中 $\alpha, \beta \in \mathfrak{o}, \beta \in M$，则 $\mathfrak{o}'$ 是Φ的含 $\mathfrak{o}$ 的一个子环，而且用定义 $\mathscr{P}'(\alpha\beta)^{-1} = \mathscr{P}(\alpha)\mathscr{P}(\beta)^{-1}$ 可把$\mathscr{P}$扩张为 $\mathfrak{o}'$到Ω内的同态$\mathscr{P}'$(导言的 I)．由于$\mathscr{P}$是极大的，故有 $\mathfrak{o}' = \mathfrak{o}$．这就是说在$\mathscr{P}$之下 $\mathfrak{o}$ 的象是Ω的一个子域 E；因为，如果 $\beta \in \mathfrak{o}$，$0 \neq \gamma = \mathscr{P}(\beta)$，则 $\beta \in M$，那么 $\beta^{-1} \in \mathfrak{o}' = \mathfrak{o}, \gamma^{-1} = \mathscr{P}(\beta^{-1})$属于 $\mathfrak{o}$ 的象．现设α是Φ的 $\neq 0$ 的任意元．我们要证明α或者 $\alpha^{-1} \in \mathfrak{o}$，这样就证明了 $\mathfrak{o}$ 是赋值环和$\mathscr{P}$是一个位．引理 1 表示 $\mathfrak{m}\mathfrak{o}[\alpha] \subset \mathfrak{o}[\alpha]$ 或者 $\mathfrak{m}\mathfrak{o}[\alpha^{-1}] \subset \mathfrak{o}[\alpha^{-1}]$，可以假设前者成立，则我们将证明$\mathscr{P}$可扩张成 $\mathfrak{o}[\alpha]$ 到Ω内的一个同态．由此和$\mathscr{P}$的极大性得 $\alpha \in \mathfrak{o}$．我们考虑多项式环 $\mathfrak{o}[x]$ 和 $E[x]$，x 为未定元，并把$\mathscr{P}$扩张成 $\mathfrak{o}[x]$到$E[x]$ 上的一个同态：$x \to x$．设 $\mathfrak{A}$ 是 $\mathfrak{o}[x]$ 中多项式 $g(x)$ 的理想，它们使得 $g(\alpha) = 0$，并设 $\mathfrak{A}'$ 是它在$\mathscr{P}$的扩张的作用下在 $E[x]$ 内的象．由于 $\mathfrak{o}[x]$ 的同态是满射的，故 $\mathfrak{A}'$ 是 $E[x]$内的一个理想，而且 $\mathfrak{A}' \subset E[x]$．否则，存在多项式 $\sum_0^{\gamma} \beta_i x^i \in \mathfrak{o}[x]$使得 $\sum \beta_i \alpha^i = 0$ 和$\sum_0^{\gamma} \mathscr{P}(\beta_i) x^i = 1$．则 $\mathscr{P}(\beta_0) = 1$，$\mathscr{P}(\beta_i) = 0$ 若 $i > 0$．故 $1 - \beta_0 \in \mathfrak{m}, \beta_i \in \mathfrak{m}$(对 $i > 0$)．故由关系式 $\sum \beta_i \alpha^i = 0$ 得 $1 = 1 - \sum \beta_i \alpha^i = (1 - \beta_0) + \sum_{i>0} (-\beta_i)\alpha^i$．由于 $1 - \beta_0, \beta_i \in \mathfrak{m}$，故 $1 \in \mathfrak{m}\mathfrak{o}[\alpha]$，这与假设矛盾．因此，$\mathfrak{A}'$ 是 $E[x]$ 中的一个真理想，因为 $E[x]$是一个主理想整区，故 $\mathfrak{A}' = (f(x))$，其中 $f(x)$ 或者是0或者是一个正次数的多项式．在第一种情况中，我们可在Ω中任选一个元 γ，在第二种情况中，可选$\gamma \in \Omega$并使 $f(\gamma) = 0$．由于Ω是代数闭域，这是可以办到的．于是γ的选择可归结为：如果 $g(x)$ 为 $\mathfrak{o}[x]$ 的满足 $g(\alpha) = 0$ 的任一多项式，则对 $E[x]$中的象 $g^{\mathscr{P}}(x)$[1]，$g^{\mathscr{P}}(\gamma) = 0$．因此，导言中的扩张定理 IV′ 表明$\mathscr{P}$可

---

1) 原文误为 $g\mathscr{P}[x]$——译者注．

扩张成 $\mathfrak{o}[\alpha]$ 到 Δ 内的一个同态，且把 α 映成 γ. 证毕.

现设 φ_0 为域 Φ 的子域 Φ_0 的一个赋值，$\mathfrak{o}_0$ 是 φ_0 的赋值环，$\mathfrak{p}_0$ 是非单位理想，U_0 是 $\mathfrak{o}_0$ 的单位的乘法群. 我们已看到 φ_0 等价于到群 Φ_0^*/U_0 内的典范赋值 φ_0'，而此群的正元是陪集 β_0U_0，$\beta_0\in\mathfrak{p}_0$，$\beta_0\neq 0$. 我们还得到被 $\mathfrak{o}_0$ 决定的 Φ_0 的典范位 $\mathscr{P}_0'$，这是一个 $\mathfrak{o}_0$ 到剩余域 $\mathfrak{o}_0/\mathfrak{p}_0$ 内的同态：$\alpha_0\to\alpha_0+\mathfrak{p}_0$. 我们可以把 $\mathfrak{o}_0/\mathfrak{p}_0$ 嵌入一个代数闭域 Ω，则 $\mathscr{P}_0'$ 可以作为 Φ_0 上的一个 Ω 值位 $\mathscr{P}_0$. 由于 Ω 是代数闭的，扩张定理断言 $\mathscr{P}_0$ 能扩张成 Φ 上的一个 Ω 值位 $\mathscr{P}$. 设 $\mathfrak{o}$ 是 Φ 内的赋值环，$\mathscr{P}$ 定义在 $\mathfrak{o}$ 上，并设 $\mathfrak{p}$ 是 $\mathfrak{o}$ 的非单位理想. 由于 $\mathscr{P}$ 是 $\mathscr{P}_0$ 的一个扩张，则 $\mathfrak{o}\supseteq\mathfrak{o}_0$，而且由于 $\mathfrak{p}$ 和 $\mathfrak{p}_0$ 分别是 $\mathscr{P}$ 和 $\mathscr{P}_0$ 的核，$\mathfrak{p}\supseteq\mathfrak{p}_0$. 因此，我们有 $\mathfrak{o}\cap\Phi_0\supseteq\mathfrak{o}_0$，$\mathfrak{p}\cap\Phi_0\supseteq\mathfrak{p}_0$. 如果 $\beta\in\mathfrak{o}\cap\Phi_0$ 和 $\beta\notin\mathfrak{o}_0$，则 $\beta^{-1}\in\mathfrak{p}_0\subseteq\mathfrak{p}$，但由此得 $\beta\notin\mathfrak{o}$. 因此 $\mathfrak{o}\cap\Phi_0=\mathfrak{o}_0$. 由于 $\mathfrak{p}$ 和 $\mathfrak{p}_0$ 分别是 $\mathfrak{o}$ 和 $\mathfrak{o}_0$ 的非单位理想，则由关系 $\mathfrak{o}\cap\Phi_0=\mathfrak{o}_0$ 推出 $\mathfrak{p}\cap\Phi_0\subseteq\mathfrak{p}_0$. 因此，$\mathfrak{p}\cap\Phi_0=\mathfrak{p}_0$，$U\cap\Phi_0=U_0$，这里 U 是 $\mathfrak{o}$ 的单位的集. 由这些关系可推得 $\beta_0U_0\to\beta_0U$，$\beta_0\in\Phi_0^*$，是有序群 Φ_0^*/U_0 到 Φ^*/U 内的一个序同构，而 Φ^*/U 被元 $\beta U(\beta\in\mathfrak{p})$ 的集所序化. 如果我们应用此同构于典范赋值 φ_0'，就得到 Φ_0 到群 Φ^*/U 内的一个等价赋值 φ_0''. 我们又有 Φ 到 Φ^*/U 内的典范赋值 φ'，并由定义知 φ' 是赋值 φ_0'' 的一个扩张. 在此意义下，我们就得到了 Φ_0 的一个给定的赋值到 Φ 上的一个赋值的扩张.

我们特别感兴趣的是 Φ 在 Φ_0 上是有限维的、而且给定的赋值是秩 1 的情况. 在一般情形，如果 φ 是域 Φ 到 $V=(G, 0)$ 内的一个赋值，则称 $\alpha(\neq 0, \alpha\in\Phi)$ 的值 $\varphi(\alpha)$ 在 G 内所成的子群为 φ 的**值群**. 我们需要下列的

引理 2. 设 φ 是域 Φ 的一个赋值，Φ_0 是 Φ 的一个有限余维数的子域，则 Φ 的值群序同构于 Φ_0 的值群的一个子群（关于 φ 的限制）.

证. 设 $\xi\in\Phi$ 并令 $\alpha_1\xi^{n_1}+\alpha_2\xi^{n_2}+\cdots+\alpha_k\xi^{n_k}=0$ 而 $\alpha_i\neq 0$，$\alpha_i\in\Phi_0$，且 $n_1>n_2>\cdots>n_k$. 如在非阿基米得实赋值的情

形一样，如果 $\varphi(\beta_1)>\varphi(\beta_i), i\neq 1$，则 $\varphi(\sum\beta_i)=\varphi(\beta_1)$。因此，由此关系推得，存在 $i<j$ 使得 $\varphi(\alpha_i\xi^{n_i})=\varphi(\alpha_j\xi^{n_j})$，则 $\varphi(\xi^{n_j-n_i})=\varphi(\alpha_j\alpha_i^{-1})$。如果 $[\Phi:\Phi_0]=n$，则可设 $n_j-n_i\leqslant n$；因此 $\varphi(\xi)^{n!}$ 是在 Φ_0 的值群内。这表明对在 Φ 的值群内的任意 a，$a^{n!}$ 是在 Φ_0 的值群 G_0 内的。另一方面，我们已知道 $a\to a^{n!}$ 是 G 到一个子群上的保序同构。故 G 是序同构于 G_0 的一个子群的。

由此结果和定理 8 得到 Φ 的值群是秩 1 的(秩 1 离散的)当且仅当对 Φ_0 的值群也如此。

现在，我们将看到如何把这一切应用于实赋值：设 φ_0 是域 Φ_0 到非负实数内的一个非平凡、非阿基米得赋值，并设 Φ 是 Φ_0 的一个有限维扩张，那么，我们知道 $\varphi_0=\varphi_0'\eta$，这里 φ_0' 是 Φ_0(它与 φ_0 的赋值环 $\mathfrak{o}_0$ 相关联)的典范赋值，η 是 φ_0' 的值群 G_0' 到正实数 P 内的一个序同构。正如刚才看到的，我们得到了 Φ 的一个赋值环 $\mathfrak{o}$ 和一个 G_0' 到典范赋值 φ' 的值群 G' 内的序同构 ζ，φ' 是由 $\mathfrak{o}$ 决定的并使得对一切 $\alpha_0\in\Phi_0$ 有 $\varphi'(\alpha_0)=(\varphi'\zeta)(\alpha_0)$。由于 G' 和 G_0' 同样是秩 1 的，所以得到一个 G' 到 P 内的序同构 λ。因此，有下列的映射图：

$$
\begin{array}{ccccc}
\Phi_0 & \xrightarrow{\varphi_0'} & G_0' & \xrightarrow{\eta} & P \\
\downarrow i & & \downarrow \zeta & & \downarrow 1 \\
\Phi & \xrightarrow[\varphi']{} & G' & \xrightarrow[\lambda]{} & P
\end{array}
$$

其中 i 是包含映射，第一个方格是交换的：$i\varphi'=\varphi_0'\zeta$。设 $G_0'\neq 1$，δ 是 G_0' 中某个 $\neq 1$ 的元，那么能选择 λ 使 $\delta^{\zeta\lambda}=\delta^{\eta}$ 并对一切 $\gamma_0'\in G_0'$ 有 $\gamma_0'^{\zeta\eta}=\gamma_0'^{\eta}$ (§10)。就是说图中的第二个方格也是交换的。所以 $\varphi=\varphi'\lambda$ 是一个实非阿基米得赋值，它是 Φ_0 上给定的赋值 φ_0 的扩张；因为如果 $\alpha_0\in\Phi_0$，则 $\varphi_0(\alpha_0)=(\varphi_0'\eta)(\alpha_0)=(\varphi_0'\zeta\lambda)(\alpha_0)\ (\varphi'\lambda)\ (\alpha_0)=\varphi(\alpha_0)$。如果 $G_0'=1$，则引理 2 表明必须有 $G'=1$。那么，η 和 λ 是唯一的且交换性成立。当然这一情形一开始就是平凡的，因为这是 φ_0 为平凡赋值的情形。因此，我们证明了下述的结论：

定理 10. 设 φ_0 是域 Φ_0 的一个非阿基米得实赋值，Φ 是 Φ_0[1]

1) 原文误为 Φ——译者注。

的一个有限维扩张域，则存在一个Φ上的实赋值，它是φ_0[1]的一个扩张。

12. 扩张定理的应用：希尔伯特零点定理 在继续研究赋值之前，我们要稍微离开主题去处理同态扩张定理（定理 9）的某些重要应用。首先，希尔伯特零点定理在代数几何中起着重要的作用。我们将以它原来的理想论的形式给此定理。

考虑域Φ上的未定元x_i的一个多项式代数$\Phi[x_1, x_2 \cdots, x_n]$，设$\Omega$是$\Phi$的代数闭包，如果$f(x_1, \cdots, x_n) \in \Phi[x_1, \cdots, x_n]$且$\xi_i$是$\Omega$的使$f(\xi_1, \cdots, \xi_n) = 0$的元，则称$(\xi_1, \cdots, \xi_n)$为$f(x_1, \cdots, x_n)$的一个(代数的)零点。设$S$是$\Phi[x_1, \cdots, x_n]$中的一个多项式集，如果$n$元组$(\xi_1, \xi_2, \cdots, \xi_n)$是每个$f(\in S)$的零点，则称$n$元组$(\xi_1, \cdots, \xi_n)$是$S$的零点。我们的主要结果是与$\Phi[x_1, \cdots, x_n]$中真素理想的零点有关的。这就是下述的

定理 11. 设$\mathfrak{P}$是$\Phi[x_1, \cdots, x_n]$的一个素理想，Φ是一个域，并设$\mathfrak{P} \neq (1)(=\Phi[x_1, \cdots, x_n])$，$g(x_1, \cdots, x_n)$是一个不在$\mathfrak{P}$中的多项式，那么在$\Phi$的代数闭包$\Omega$中存在$\xi_i$使得$(\xi_1, \cdots, \xi_n)$对$\mathfrak{P}$是一个零点但不是$g(x_1, \cdots, x_n)$的零点。

证. 由于$\mathfrak{P} \neq (1)$，$\Phi[x_1, \cdots, x_n]/\mathfrak{P}$是$\Phi$上$(\neq 0)$的代数，它是由陪集$\gamma_i = x_i + \mathfrak{P} (i = 1, 2, \cdots, n)$在$\Phi$上生成的，而且$\Phi[\gamma_1, \cdots, \gamma_n] = \Phi[x_1, \cdots, x_n]/\mathfrak{P}$是一个整区，故能把它嵌入它的分式域$P = \Phi(\gamma_1, \cdots, \gamma_n)$中。首先设一切$\gamma_i$都是代数的，那么P是$\Phi$的代数扩张，故存在$P/\Phi$到代数闭包$\Omega/\Phi$内的一个同构。设此同构为：$\gamma_i \to \xi_i$。那么，如果$f(x_1, \cdots, x_n) \in \mathfrak{P}$，$f(\gamma_1, \cdots, \gamma_n) = 0$因而$f(\xi_1, \cdots, \xi_n) = 0$，故$(\xi_1, \cdots, \xi_n)$是$\mathfrak{P}$的一个零点。另一方面，$g(x_1, \cdots, x_n) \notin \mathfrak{P}$，故$g(\gamma_1, \cdots, \gamma_n) \neq 0$；因此，$g(\xi_1, \cdots, \xi_n) \neq 0$。在这种情形下定理成立。其次，设不是所有的$\gamma_i$都是代数的，可把$\gamma_i$这样排列使得$\{\gamma_1, \cdots, \gamma_r\}$

1) 原文误为φ——译者注。

$(r \geqslant 1)$ 是 P/Φ 的一个超越基。由于 $g(x_1, \cdots, x_n) \notin \mathfrak{P}$，在 P 中 $g(\gamma_1, \cdots, \gamma_n) \neq 0$，故在 P 中 $g(\gamma_1, \cdots, \gamma_n)^{-1}$ 存在。此元和 $\gamma_{r+1}, \cdots, \gamma_n$ 诸元在 $\Phi(\gamma_1, \cdots, \gamma_r)$ 上是代数的，故满足形如下述的代数方程

$$(35) \qquad a_0(\gamma_1, \cdots, \gamma_r)x^m + a_1(\gamma_1, \cdots, \gamma_r)x^{m-1} + \cdots + a_m(\gamma_1, \cdots, \gamma_r) = 0,$$

其中 a_i 是 γ_j 的多项式 $(j = 1, \cdots, r)$，$a_0(\gamma_1, \cdots, \gamma_r) \neq 0$。对每个 $\gamma_{r+1}, \cdots, \gamma_n$ 和 $g(\gamma_1, \cdots, \gamma_n)^{-1}$ 可选择这样一个方程，并令 $a(\gamma_1, \cdots, \gamma_r)$ 为这些方程首项系数的积。由于 $a(\gamma_1, \cdots, \gamma_r) \neq 0$，在无限域 Ω 中可选取 $\xi_1, \cdots, \xi_r$ 使得 $a(\xi_1, \cdots, \xi_r) \neq 0$（卷 1，中译本 p.104）。由于 $\gamma_j, 1 \leqslant j \leqslant r$，是代数无关的，故存在一个由 $\Phi[\gamma_1, \cdots, \gamma_r]$ 到 Ω/Φ 内的代数同态使得 $\gamma_j \to \xi_j$。由扩张定理（定理 9），此同态能扩张成 P 上的一个 Ω 值位 $\mathscr{P}$。由于 $\mathscr{P}$ 是一个代数同态的扩张，则 $\mathscr{P}$ 在 Φ 上是恒等的，故 $\mathscr{P}$ 是到 Ω/Φ 内的一个代数同态。我们其次还要注意，$\gamma_k (r+1 \leqslant k \leqslant n)$ 在 $\mathscr{P}$ 的赋值环 $\mathfrak{o}$ 内。否则，$\mathscr{P}(\gamma_k^{-1}) = 0$。另方面，我们有一个方程形如

$$a_0(\gamma_1, \cdots, \gamma_r) + a_1(\gamma_1, \cdots, \gamma_r)\gamma_k^{-1} + \cdots + a_m(\gamma_1, \cdots, \gamma_r)\gamma_k^{-m} = 0,$$

并用 $\mathscr{P}$ 作用得到 $a_0(\xi_1, \cdots, \xi_r) = \mathscr{P}(a_0(\gamma_1, \cdots, \gamma_r)) = 0$。这与下述事实矛盾：$a(\xi_1, \cdots, \xi_r) \neq 0$ 且 $a_0(\gamma_1, \cdots, \gamma_r)$ 是 $a(\gamma_1, \cdots, \gamma_r)$ 的一个因式。同法可证 $\mathscr{P}(g(\gamma_1, \cdots, \gamma_n)) \neq 0$。令 $\xi_k = \mathscr{P}(\gamma_k)(r+1 \leqslant k \leqslant n)$，则我们断言 $(\xi_1, \cdots, \xi_n)$ 满足定理的条件：首先，若 $f(x_1, \cdots, x_n) \in \mathfrak{P}$，则 $f(\gamma_1, \cdots, \gamma_n) = 0$ 且施行 $\mathscr{P}$ 得 $f(\xi_1, \cdots, \xi_n) = 0$。其次，有 $g(\xi_1, \cdots, \xi_n) = \mathscr{P}(g(\gamma_1, \cdots, \gamma_n)) \neq 0$。

希尔伯特零点定理是定理 11 在 $\Phi[x_1, \cdots, x_n]$ 中由素理想到任意理想的推广。为此，我们需要交换环中一个理想的（诣零）根之刻划（卷 1，中译本 p.161）。我们需要的结果是：如果 $\mathfrak{A}$ 是交换环 $\mathfrak{o}$ 的一个理想，则根 $\mathfrak{R}(\mathfrak{A})$ 是包含 $\mathfrak{A}$ 的素理想 $\mathfrak{P}$ 的交 $\cap \mathfrak{P}$。如果 $\mathfrak{o}$ 是诺特环，此结果是把理想分解为准素理想之交的

分解定理之简单推论（卷 1，中译本，p.163，习题 67 的第 2 题，p.168）. 虽然这就是我们所需要的全部了，但在一般情形下建立此结果仍是很有趣的. 我们首先证明下述的

引理 1. 设 $\mathfrak{o}$ 是交换环，$\mathfrak{A}$ 是 $\mathfrak{o}$ 的一个理想，S 是 $\mathfrak{o}$ 的一个非空乘法封闭子集使得 $\mathfrak{A}\cap S=\varnothing$. 则在 $\mathfrak{o}$ 中存在素理想 $\mathfrak{P}$ 使得 $\mathfrak{P}\supseteq\mathfrak{A}$ 且 $\mathfrak{P}\cap S=\varnothing$.

证. 设 U 是 $\mathfrak{o}$ 中理想 $\mathfrak{B}$ 的类，满足：1. $\mathfrak{B}\supseteq\mathfrak{A}$，2. $\mathfrak{B}\cap S=\varnothing$. 由于 $\mathfrak{A}\in U$，故 U 非空. 以包含关系序化 U 的元. 设 V 为 U 的一个线性序子集，$\mathfrak{C}=\bigcup\mathfrak{B}$. 则 $\mathfrak{B}\varepsilon V\mathfrak{C}\cap S=\varnothing$ 且 $\mathfrak{C}\supseteq\mathfrak{A}$. 而且，容易验证 $\mathfrak{C}$ 是一个理想. 因此 $\mathfrak{C}\in U$ 且 $\mathfrak{C}$ 是集 V 的一个上界，故 U 是个归纳集，那么能用卓伦引理推得：U 包含一个极大元 $\mathfrak{P}$. 设 $a_i, i=1,2$, 是 $\mathfrak{o}$ 的元但不含于 $\mathfrak{P}$，则由 a_i 和 $\mathfrak{P}$ 生成的理想 $\mathfrak{A}_i$ 真包含 $\mathfrak{P}$ 且包含 $\mathfrak{A}$. 由于 $\mathfrak{P}$ 在 U 内为极大元，由此得 $\mathfrak{A}_i\notin U$，这就是说 $\mathfrak{A}_i\cap S\neq\varnothing$. 设 $s_i\in\mathfrak{A}_i\cap S$，如果我们注意到 $\mathfrak{A}_i$ 的元的形式，则 $s_i=x_ia_i+p_i$，其中 $x_i\in\mathfrak{o}, p_i\in\mathfrak{P}$，那么

$$s=s_1s_2=x_1x_2a_1a_2+p, \tag{36}$$

其中 $p\in\mathfrak{P}$. 由于 S 是乘法封闭的，故 $s\in S$. 如果 $a_1a_2\in\mathfrak{P}$，则由 (36) 得到 $s\in\mathfrak{P}$，但这与 $\mathfrak{P}\cap S=\varnothing$ 矛盾，因此 $a_1a_2\notin\mathfrak{P}$，这就证明了 $a_1\notin\mathfrak{P}$, $a_2\notin\mathfrak{P}$ 蕴涵着 $a_1a_2\notin\mathfrak{P}$. 故 $\mathfrak{P}$ 是一个满足所要求条件的素理想.

现在我们可以证明

定理 12. 设 $\mathfrak{A}$ 是交换环 $\mathfrak{o}$ 的一个理想，则根 $\mathfrak{R}(\mathfrak{A})=\bigcap\mathfrak{P}$，即包含 $\mathfrak{A}$ 的素理想 $\mathfrak{P}$ 的交.

证. 设 $a\in\mathfrak{R}(\mathfrak{A})$，$\mathfrak{P}$ 为包含 $\mathfrak{A}$ 的素理想. 适当的幂 $a^n\in\mathfrak{A}$，因而 $a^n\in\mathfrak{P}$. 由于 $\mathfrak{P}$ 是素理想，由此可得 $a\in\mathfrak{P}$. 因此对包含 $\mathfrak{A}$ 的素理想 $\mathfrak{P}$ 有 $\mathfrak{R}(\mathfrak{A})\subseteq\mathfrak{P}$, $\mathfrak{R}(\mathfrak{A})\subseteq\bigcap\mathfrak{P}$. 其次，设 $a\notin\mathfrak{R}(\mathfrak{A})$ 和 $S=\{a^n, n=1,2,\cdots\}$，则 $S\cap\mathfrak{A}=\varnothing$ 且 S 是乘法封闭的，因此，由引理推出存在包含 $\mathfrak{A}$ 的素理想 $\mathfrak{P}$ 使得 $a\notin\mathfrak{P}$，故 a 不在含 $\mathfrak{A}$ 的诸素理想之交中. 这就证明了 $\bigcap\mathfrak{P}\subseteq\mathfrak{R}(\mathfrak{A})$，加上前面的包含关系有 $\mathfrak{R}(\mathfrak{A})=\bigcap\mathfrak{P}$.

由定理 11 和 12 得

希尔伯特零点定理. 设 $\mathfrak{A}$ 是多项式代数 $\Phi[x_1, x_2, \cdots, x_n]$ 中的一个理想，Φ 是一个域，x_i 为未定元，并设 Ω 是 Φ 的代数闭包，则多项式 $g(x_1, \cdots, x_n) \in \mathfrak{R}(\mathfrak{A})$ 当且仅当对想理 $\mathfrak{A}$ 的每个零点 $(\xi_1, \cdots, \xi_n)(\xi_i \in \Omega)$ 有 $g(\xi_1, \cdots, \xi_n) = 0$.

证. 设 V 表示 $\mathfrak{A}$ 的诸零点 $(\xi_1, \cdots, \xi_n)$ 的集，$\xi_i \in \Omega$. 设 $g(x_1, \cdots, x_n) \in \mathfrak{R}(\mathfrak{A})$，则对某个正整数 n，$g^n \in \mathfrak{A}$. 因此对每个$(\xi_i) \in V$，$g(\xi_1, \cdots, \xi_n)^n = 0$，且对每个 $(\xi_i) \in V$，$g(\xi_1, \cdots, \xi_n) = 0$. 反之，设 $g(x_1, \cdots, x_n)$ 是一个多项式使得对每个 $(\xi_i) \in V$ 有 $g(\xi_1, \cdots, \xi_n) = 0$. 设 $\mathfrak{P}$ 是含 $\mathfrak{A}$ 的素理想，并设W为 $\mathfrak{P}$ 的诸零点的集，由于 $\mathfrak{P} \supseteq \mathfrak{A}$ $W \subseteq V$，所以对每个$(\xi_i) \in W$有 $g(\xi_1, \cdots, \xi_n) = 0$. 由定理 11 得到 $g(x_1, \cdots, x_n) \in \mathfrak{P}$. 因此，含 $\mathfrak{A}$ 的每个素理想均包含 g，那么由定理 12，$g \in \mathfrak{R}(\mathfrak{A})$. 证毕.

其次，我们将把素理想代数零点的存在性应用到关于域的有限生成的一个定理上去. 我们早就知道 (§1.5，引理 2)，如果 $\gamma_1, \cdots, \gamma_n$ 在 Φ 上是代数的，则域 $\mathrm{P} = \Phi(\gamma_1, \cdots, \gamma_n)$ 同由各γ_i 生成的代数 $\Phi[\gamma_1, \cdots, \gamma_n]$ 是一致的. 我们可以证明此结果的下述逆定理.

定理 13. 如果Φ上的由 γ_i 生成的代数$\mathrm{P} = \Phi[\gamma_1, \gamma_2, \cdots, \gamma_n]$ 是个域，则各 γ_i 在 Φ 上是代数的.

证. 设 $\Phi[x_1, \cdots, x_n]$ 是Φ上的含未定元 x_i 的多项式代数，并考虑此代数到 P/Φ 上的同态 $x_i \to \gamma_i$，$1 \leqslant i \leqslant n$. 设 $\mathfrak{P}$ 是同态的核，由于P是一个域，所以 $\mathfrak{P}$ 是一个极大理想. 如果Ω是Φ的代数闭包，则我们可以找到 $(\xi_1, \cdots, \xi_n) \in \Omega$ 使得对每个 $f \in \mathfrak{P}$ 有 $f(\xi_1, \cdots, \xi_n) = 0$. 由导言的 IV，存在$\Phi$上的 $\mathrm{P} = \Phi[\gamma_1, \gamma_2, \cdots, \gamma_n]$ 到 $\Phi[\xi_1, \xi_2, \cdots, \xi_n]$ 上的一个同态使得 $\gamma_i \to \xi_i$，$1 \leqslant i \leqslant n$. 由于P是一个域，此同态是一个同构. 由于 ξ_i 是代数的，故 γ_i 也是代数的，$1 \leqslant i \leqslant n$.

习 题 42

1. 设 $\mathrm{P} = \Phi[\gamma_1, \gamma_2, \cdots, \gamma_n]$ 是Φ上的有限生成交换代数，$\mathfrak{R}$ 是幂零元的理想，证明

$\mathfrak{R}$ 是 $\mathfrak{P}$ 的极大理想的交.

13. 扩张定理的应用：整闭包 下面我们将应用扩张定理去得到一个域的子域的整闭包的重要刻划. 设 $\mathfrak{g}$ 是域 Φ 的一个子环. 我们记得一个元 $\alpha \in \Phi$ 为关于 $\mathfrak{g}$ 是整的或 $\mathfrak{g}$ 整的，如果存在多项式 $f(x) \in \mathfrak{g}[x]$，其首项系数为 1，使得 $f(\alpha) = 0$. Φ 中 $\mathfrak{g}$ 整元的集 $\mathfrak{G}$ 被称为 $\mathfrak{g}$ 在 Φ 中的整闭包. 我们将刻划这个集. 证明中需要下述的

引理 1. 如果 $\mathfrak{o}$ 是一个交换环（有单位元 1），则 $\mathfrak{o}$ 的任何真理想 $\mathfrak{A}$ 均能嵌入一个极大理想之中.

证. 本引理的证明可作为 §12 引理 1 的证明之特殊情况得到. 令 $S = \{1\}$，那么 S 是乘法封闭的且 $S \cap \mathfrak{A} = \varnothing$. 设 U 是理想 $\mathfrak{B}$ 的集，而 $\mathfrak{B}$ 满足：$\mathfrak{B} \supseteq \mathfrak{A}$ 且 $\mathfrak{B}$ 是真理想（所以 $\mathfrak{B} \cap S = \varnothing$）. 则 U 包含一个极大元 $\mathfrak{P}$. 直接可得 $\mathfrak{P}$ 是含 $\mathfrak{A}$ 的一个极大理想.

定理 14（克鲁尔）. 设 $\mathfrak{g}$ 是域 Φ 中含 1 的子环，则 $\mathfrak{g}$ 在 Φ 中的整闭包 $\mathfrak{G}$ 是 $\cap \mathfrak{o}$，即 Φ 中含 $\mathfrak{g}$ 的一切赋值环的交.

证. 设 $\alpha \in \mathfrak{G}$，我们有关系式 $\alpha^n + \gamma_1\alpha^{n-1} + \cdots + \gamma_n = 0$，$n \geqslant 1$，$\gamma_i \in \mathfrak{g}$. 设 φ 是一个赋值，它的赋值环 $\mathfrak{o}$ 包含 $\mathfrak{g}$. 如果 $\alpha \notin \mathfrak{o}$，则 $\varphi(\alpha^{-1}) < 1$. 但 $1 = -\gamma_1\alpha^{-1} - \cdots - \gamma_n\alpha^{-n}$ 且 $\varphi(\gamma_i) \leqslant 1$，因此，每个 $\varphi(\gamma_i\alpha^{-1}) < 1$，但这是不可能的. 因为由此关系式可得 $1 = \varphi(1) \leqslant \max(\varphi(\gamma_i\alpha^{-1})) < 1$. 因此，$\alpha \in \mathfrak{o}$，于是我们证明了 $\mathfrak{G}$ 含于 $\cap \mathfrak{o}$，这里的赋值环 $\mathfrak{o}$ 包含 $\mathfrak{g}$. 其次，假设 $\alpha \notin \mathfrak{G}$，则 α^{-1} 在环 $\mathfrak{g}[\alpha^{-1}]$ 中不是一个单位，因为否则它的逆 $\alpha = \gamma_0 1 + \gamma_1\alpha^{-1} + \cdots + \gamma_{n-1}\alpha^{-(n-1)}$，$\gamma_i \in \mathfrak{g}$，因此 $\alpha^n = \gamma_0\alpha_0^{n-1} + \gamma_1\alpha^{n-2} + \cdots + \gamma_{n-1}$，那么 $\alpha \in \mathfrak{G}$. 由于 α^{-1} 不是 $\mathfrak{g}[\alpha^{-1}]$ 中的单位，则主理想 $\alpha^{-1}\mathfrak{g}[\alpha^{-1}]$ 是真包含在 $\mathfrak{g}[\alpha^{-1}]$ 中. 由引理 1，在 $\mathfrak{g}[\alpha^{-1}]$ 中存在一个含 $\alpha^{-1}\mathfrak{g}[\alpha^{-1}]$ 的极大理想 $\mathfrak{m}$，故 $\mathfrak{g}[\alpha^{-1}]/\mathfrak{m}$ 是一个域，并可把它嵌入一个代数闭域 Ω 内. $\mathfrak{g}[\alpha^{-1}]$ 到 $\mathfrak{g}[\alpha^{-1}]/\mathfrak{m}$ 上的典范同态可以被看成 $\mathfrak{g}[\alpha^{-1}]$ 到 Ω 内的一个同态. 由扩张定理得到一个 Ω 值位 $\mathscr{P}$，它的赋值环 $\mathfrak{o}$ 包含 $\mathfrak{g}[\alpha^{-1}]$. $\mathfrak{o}$ 的非单位所成的理想 $\mathfrak{p}$ 包

含 $\mathfrak{m}$，因此含有 α^{-1}. 由此得 $\alpha \notin \mathfrak{o}$. 因此由 $\alpha \notin \mathfrak{G}$ 可得 $\alpha \notin \bigcap \mathfrak{o}$,这里的 $\mathfrak{o}$ 是包含 $\mathfrak{g}$ 的赋值环. 所以,我们有 $\mathfrak{G} = \bigcap \mathfrak{o}$. 证毕.

如果 $\mathfrak{G} = \mathfrak{g}$,则称子环 $\mathfrak{g}$ 在 Φ 中是整闭的. 故我们有下述的结论

推论. 如果 $\mathfrak{g}$ 是 Φ 的一个子环,则 $\mathfrak{g}$ 整元的集 $\mathfrak{G}$ 是 Φ 中包含 $\mathfrak{g}$ 的子环,而且 $\mathfrak{G}$ 在 Φ 中是整闭的.

证　由于 $\mathfrak{G}$ 是 Φ 的子环的交,而且 $\mathfrak{G}$ 必然包含 $\mathfrak{g}$,所以第一个断言是显然的. $\mathfrak{G}$ 整元的集是含 $\mathfrak{G}$ 的诸赋值环的交 $\bigcap \mathfrak{o}$, 故包含 $\mathfrak{g}$. 另一方面,如果 $\mathfrak{o}$ 是含 $\mathfrak{g}$ 的一个赋值环, 则 $\mathfrak{o} \supseteq \mathfrak{G}$, 因此, 含 $\mathfrak{G}$ 的诸赋值的交与含 $\mathfrak{g}$ 的诸赋值环的交相同,所以就是 $\mathfrak{G}$. 故 $\mathfrak{G}$ 是整闭的.

习　　题　　43

1.(阿廷). 设 $\mathfrak{g}$ 是域的一个子环, $\alpha_1, \alpha_2, \cdots, \alpha_r$ 是 Φ 的元. 假设对每个 i,存在正整数 n_i 使得 $\alpha_i^{n_i} = P_i(\alpha_1, \alpha_2, \cdots, \alpha_r)$,其中 P_i 是一个总次数 $< n_i$ 的多项式. 证明每个 α_i 是 $\mathfrak{g}$ 整的.

2.(阿廷). 设 $\mathfrak{g}$ 如第 1 题,并设 $\mathfrak{M}$ 是 Φ 的子环, $\mathfrak{M}$ 是有限生成 $\mathfrak{g}$ 模,证明 $\mathfrak{M}$ 的每个元是 $\mathfrak{g}$ 整的(参考卷1,中译本, p. 168).

3. 一个交换整区 $\mathfrak{g}$ 称为整闭的,如果在它的分式域中是整闭的. 证明如果 $\mathfrak{g}$ 是高斯整区(即唯一因子分解成立),则 $\mathfrak{g}$ 是整闭的.

4.(柯恩). 设 Φ 为域, x 为未定元,证明 $\Phi[x]$ 的子代数 $\mathfrak{A}$ 有单一生成元当且仅当 $\mathfrak{A}$ 是整闭的. (提示: 使用吕洛斯定理和定理14.)

14. 完备域的有限维扩张　在本章剩下的部分中,我们回过头来考虑实赋值(阿基米得的与非阿基米得的). 开始, 我们将考虑把完备域 Φ 上的赋值扩充到有限维扩张域的问题. 我们的首要目标是证明扩张的唯一性. 为此,我们要求

引理 1. 设 Φ 关于非平凡实赋值 φ 是完备的, 并设 P 是 Φ 的一个扩张域,具有赋值 φ,它是 Φ 之赋值的一个扩张. 设 $u_1, u_2, \cdots, u_r$ 是 P 的元而且是 Φ 一无关的. 则序列 $\{a_n\}$($a_n = \sum_{i=1}^{r} \alpha_{ni} u_i$, $\alpha_{ni} \in \Phi$) 是 P 中的柯西序列当且仅当这 r 个序列 $\{\alpha_{ni}\}$($i = 1, 2, \cdots, r$) 是 Φ 中的柯西序列.

证. 如果 $\{\alpha_{ni}\}$ 是柯西序列则可直接得到 $\{a_n\}$ 也是;反之,设 $\{a_n\}$ 是柯西序列. 如果 $r=1$,则显然 $\{\alpha_{ni}\}$ 是柯西序列. 现在我们将对任意 r 用归纳法证明我们的断言, 如果序列 $\{\alpha_{nr}\}$ 是一个柯西序列,则序列 $\{b_n\}$,$b_n=a_n-\alpha_{nr}u_r$, 是一个柯西序列. 由于 $b_n=\sum_{1}^{r-1}\alpha_{nj}u_j$,所要求的结果可由归纳法得到. 如果能证明,在 $\{\alpha_{nr}\}$ 不是柯西序列的假设下能导致矛盾, 那么我们就完成了此题的证明. 我们设 $\{\alpha_{nr}\}$ 不是柯西序列, 则存在实数 $\varepsilon>0$, 使得对任意正整数N存在 $p, q>N$ 有 $\varphi(\alpha_{pr}-\alpha_{qr})>\varepsilon$. 因此存在正整数对 (p_k,q_k),$p_1<p_2<\cdots$,$q_1<q_2<\cdots$,使得$\varphi(\alpha_{p_kr}-\alpha_{q_kr})>\varepsilon$. 那么 $(\alpha_{p_kr}-\alpha_{q_kr})^{-1}$ 存在并作出序列 $\{b_k\}$, 其中

$$b_k=(\alpha_{p_kr}-\alpha_{q_kr})^{-1}(a_{p_k}-a_{q_k}). \tag{37}$$

我们有 $\varphi(\alpha_{p_kr}-\alpha_{q_kr})^{-1}<\dfrac{1}{\varepsilon}$,$\{a_{p_k}-a_{q_k}\}$ 是零序列, 因此 $\{b_k\}$ 是零序列. 另一方面, $b_k=\sum_{j=1}^{r-1}\beta_{kj}u_j+u_r$,并由此得, 如果 $c_k=\sum\beta_{kj}u_j$,则 $\{c_k\}$ 是柯西序列. 那么,这 $r-1$ 个序列 $\{\beta_{kj}\}$,$j=1,2,\cdots,r-1$, 是柯西序列. 由于Φ是完备的, $\lim\beta_{kj}=\beta_j$ 存在. 因为 $\lim b_k=0$,从 $b_k=\sum_{1}^{r-1}\beta_{kj}u_j+u_r$得到$0=\sum_{1}^{r-1}\beta_ju_j+u_r$. 这与诸 u_i 的线性无关性矛盾. 证毕.

要注意此引理的两个重要结果: (1) 如果 $\{a_n\}$ 是一个零序列,则这一切序列 $\{\alpha_{ni}\}$ 都是零序列. (2) 如果 $[\mathrm{P}:\Phi]<\infty$, 则 P 是完备的. 由于 $\{\alpha_{ni}\}$ 都是柯西序列, 第一个命题是显然的. 因此 $\lim\alpha_{ni}=\alpha_i$ 存在且 $\sum\alpha_iu_i=0$. 因此,由 u_i 的线无关性性得每个 $\alpha_i=0$. 为了证明第二个命题,我们设 $(u_1,u_2,\cdots,u_r)$ 是一个基,那么,如果 $\{a_n\}$ 是柯西序列, 则每个 $\{\alpha_{ni}\}$ 也是柯西序列,因此 $\lim\alpha_{ni}=\alpha_i$ 存在,而且 $\lim a_n=\sum\alpha_iu_i$.

现在,我们可以证明

定理 15. 设 P 是一个域的有限维扩张域,而该域关于非平凡

实赋值 φ 是完备的．那么，如果 φ 能扩张成 P 的一个实赋值，则此赋值是唯一的并由下列公式给出：

$$\varphi(\rho)=\varphi(N_{P|\Phi}(\rho))^{1/n},\quad n=[P:\Phi]. \tag{38}$$

证．设扩张 φ 存在，并设存在 $\rho\in P$ 使得 (38) 不成立，则 $\varphi(\rho^n)\neq\varphi(N(\rho))$，于是 $\rho\neq 0$，而且 $\varphi(\rho^n)<\varphi(N(\rho))$ 或者 $\varphi(\rho^n)>\varphi(N(\rho))$．若必要，可用 ρ^{-1}代替 ρ，故可设 $\varphi(\rho^n)<\varphi(N(\rho))$．令 $\sigma=\rho^n N(\rho)^{-1}$，则 $\varphi(\sigma)<1$ 和 $N(\sigma)=N(\rho^n)\cdot N(\rho)^{-n}=1$．因为 $\varphi(\sigma)<1$，故 $\lim\sigma^k=0$．如果 $(u_1,u_2,\cdots,u_n)$ 是一个基，$\sigma^k=\sum_{i=1}^{n}\alpha_{ki}u_i$，则由 $\lim\alpha^k=0$ 得 $\lim\alpha_{ki}=0$，对每个 i．因为元 $\varepsilon=\sum\gamma_i u_i$ $(\gamma_i\in\Phi)$ 的范数是 γ_i 的具有固定系数的多项式，显然由 $\lim\alpha_{ki}=0$（对每个 i）可得 $\lim N(\sigma^k)=0$．这与 $N(\sigma^k)=N(\sigma)^k=1$ 矛盾．

前面我们已看到一个子域上的任意非阿基米得实赋值均可扩张，因此在非阿基米得的情形，公式(38)为有限维扩张域 P 提供了一个赋值；剩下来的是考虑阿基米得的情形．在此情形，将通过完全决定所有关于一个阿基米得实赋值完备的域来得出扩张定理．我们将证明这样的域仅有实数域和复数域．

引理 2. 设 P 是域 Φ 的二次扩张，而 Φ 关于实阿基米得赋值 φ 是完备的，则 φ 可以扩张成 P 的赋值．

证　我们知道，阿基米得实赋值的存在意味着特征是 0[1]，因此 P 是 Φ 上的伽罗瓦域．设 $\alpha\to\bar{\alpha}$ 是 P/Φ 的自同构，它不是恒等的，则对 $\alpha\in P$ 的迹和范数是 $T(\alpha)=\alpha+\bar{\alpha}$，$N(\alpha)=\alpha\bar{\alpha}$，而且对任何 $\alpha\in P$ 有 $\alpha^2-T(\alpha)\alpha+N(\alpha)=0$．我们将证明 $\varphi(\alpha)=\varphi(N(\alpha))^{1/2}$定义 P 的一个赋值．如 $\alpha\in\Phi$，则 $N(\alpha)=\alpha^2$，这意味着定义在 P 上的映射是 Φ 上给定的 φ 的一个扩张．显然有：仅当 $\alpha=0$ 时 $\varphi(\alpha)=0$，而且由范数的乘法性质推出 $\varphi(\alpha\beta)=\varphi(\alpha)\varphi(\beta)$．因此，只需证明 $\varphi(\alpha+\beta)\leqslant\varphi(\alpha)+\varphi(\beta)$ 就行了．

---

1) 指 Φ 的特征为 0——译者注．

如果我们能证明 $\varphi(\alpha+1)\leqslant\varphi(\alpha)+1$，则此式可得．因为，若 $\beta=0$，显然有 $\varphi(\alpha+\beta)\leqslant\varphi(\alpha)+\varphi(\beta)$；如果 $\beta\neq 0$，则

$$\varphi(\alpha+\beta)=\varphi((\alpha\beta^{-1}+1)\beta)=\varphi(\alpha\beta^{-1}+1)\varphi(\beta).$$

因此，如果 $\varphi(\alpha\beta^{-1}+1)\leqslant\varphi(\alpha\beta^{-1})+1$，则

$$\varphi(\alpha+\beta)\leqslant(\varphi(\alpha\beta^{-1})+1)\varphi(\beta)=(\varphi(\alpha)\varphi(\beta)^{-1}+1)\varphi(\beta)$$
$$=\varphi(\alpha)+\varphi(\beta).$$

现在，如果 $\alpha\in\Phi$，$\varphi(\alpha+1)\leqslant\varphi(\alpha)+1$ 成立；故我们设 $\alpha\notin\Phi$，则 $\mathrm{P}=\Phi(\alpha)$，$x^2-T(\alpha)x+N(\alpha)$ 是 α 的最小多项式，而且 $N(\alpha+1)=(\alpha+1)(\bar\alpha+1)=\alpha\bar\alpha+\alpha+\bar\alpha+1=N(\alpha)+T(\alpha)+1$． 因此 $\varphi(\alpha+1)\leqslant\varphi(\alpha)+1$ 是等价于 $\varphi(\alpha+1)^2\leqslant\varphi(\alpha)^2+2\varphi(\alpha)+1$ 并等价于

$$\varphi(1+T(\alpha)+N(\alpha))\leqslant 1+2\varphi(N(\alpha))^{1/2}+\varphi(N(\alpha)). \tag{39}$$

如果我们应用 φ 在 Φ 中的加法性质，则易得：如果 $\varphi(T(\alpha))\leqslant 2\varphi(N(\alpha))^{1/2}$，那么 (39) 成立． 所以，我们设 $\varphi(T(\alpha))>2\varphi(N(\alpha))^{1/2}$，或者 $\varphi(T(\alpha))^2>4\varphi(N(\alpha))$．如果记 $a=T(\alpha)$，$b=N(\alpha)$，那么我们的假设就变成 $\varphi(a)^2>4\varphi(b)$． 我们将证明，由此可推得 $\alpha\in\Phi$，从而与我们的假设矛盾．因此，要完成本定理的证明，就需要证明

引理 3. 设 Φ 是关于实赋值 φ 的一个完备域，并设 $x^2-ax+b=0$ 是一个方程，其系数 $a,b\in\Phi$ 使得 $\varphi(a)^2>4\varphi(b)$，则此方程在 Φ 内有根．

证．此方程的一个非零根 α 将是 $\alpha=a-b\alpha^{-1}$ 的一个根，这个根将作序列 $\{a_n\}$ 的极限得到，其中 a_n 是递推地定义的：$a_1=\frac{1}{2}a$，$a_{n+1}=a-ba_n^{-1}$．我们首先证明没有 $a_n=0$，从而对一切 n 定义是有效的．我们有 $\varphi(a_1)=\frac{1}{2}\varphi(a)>0$，我们可以假定 $\varphi(a_n)\geqslant\frac{1}{2}\varphi(a)$，则

$$\varphi(a_{n+1}) = \varphi(a - ba_n^{-1}) \geqslant \varphi(a) - \varphi(b)\varphi(a_n)^{-1}$$
$$\geqslant \varphi(a) - 2\varphi(b)\varphi(a)^{-1}$$
$$\geqslant \varphi(a) - \frac{1}{2}\varphi(a)^2\varphi(a)^{-1} = \frac{1}{2}\varphi(a).$$

因此,对一切 $n = 1,2,3,\cdots$, $\varphi(a_n) \geqslant \frac{1}{2}\varphi(a) > 0$, 而且每个 $a_n \neq 0$. 今有 $a_{n+2} - a_{n+1} = ba_{n+1}^{-1}a_n^{-1}(a_{n+1} - a_n)$; 而且 $\varphi(a_{n+1})^{-1}\varphi(a_n)^{-1} \leqslant 4\varphi(a)^{-2}$;因此

$$\varphi(a_{n+2} - a_{n+1}) \leqslant \frac{4\varphi(b)}{\varphi(a)^2}\varphi(a_{n+1} - a_n). \tag{40}$$

如果令 $r = 4\varphi(b)/\varphi(a)^2$, 则 $0 \leqslant r < 1$, 而且反复用 (40) 得 $\varphi(a_{n+2} - a_{n+1}) \leqslant r^n c$,其中 $c = \varphi(a_2 - a_1)$. 由此不等式容易推出 $\{a_n\}$ 是一个柯西序列. 因此 $\alpha = \lim a_n$ 存在,且由于 $\varphi(a_n) \geqslant \frac{1}{2}\varphi(a) > 0$,有 $\alpha \neq 0$. 所以, 由递推公式 $a_{n+1} = a - ba_n^{-1}$ 得到 $\alpha = a - b\alpha^{-1}$,故 $\alpha^2 - a\alpha + b = 0$.

现在我们着手证明

定理 16 (奥斯特洛夫斯基 (Ostrowski)). 关于一个实阿基米得赋值完备的域仅有实数域和复数域.

证 设 Φ 关于阿基米得赋值 φ 是完备的. 则 Φ 的特征为 0, 那么它包含有理数. 由于有理的任一个实阿基米得赋值等价于绝对值赋值且 Φ 是完备的, 故显然 Φ 包含实数域. 如果 Φ 包含一个元 i 使得 $i^2 = -1$,则 Φ 包含复数域 C. 否则, 添加 i 到 Φ 得到 $\Phi(i)$ 包含 C. 由引理 2,可以把 φ 扩张成 $\Phi(i)$ 的实赋值. 我们知道 $\Phi(i)$ 是完备的. 因此, 要得到此定理, 只需要证明下述命题: 如果 Φ 关于一个阿基米得赋值是完备的,而且 $\Phi \supseteq C$,则 $\Phi = C$. 由于 φ 在实子域(有理数的完备化) 上的限制等价于绝对值赋值,定理 15 表明 φ 等价于 C 上的绝对赋值.

现在设 $\Phi \supset C$, $\alpha \in \Phi$, $\notin C$. 设 $r = \inf\varphi(\alpha - c)$,对 $c \in C$. 则我们断言存在一个 $c_0 \in C$ 使得 $\varphi(\alpha + c_0) = r$. 首先,显然对

一切使得 $\varphi(\alpha-c)\leqslant r+1$，而且当 c_1 和 c_2 是两个复数满足 $\varphi(\alpha-c_1)\leqslant r+1, \varphi(\alpha-c_2)\leqslant r+1$，则 $\varphi(c_1-c_2)\leqslant 2r+2$，所以满足 $\varphi(\alpha-c)\leqslant r+1$ 的 c 之集在 C 中是封闭的和有界的。因为 $\varphi(\alpha-c)$ 是 c 的连续函数，显然存在 c_0 使 $\varphi(\alpha-c_0)=r$。由于 $\alpha\notin C$ 我们有 $r>0$。如果用 $\alpha-c_0$ 代替 α，可假定 $c_0=0$。则我们有 $\varphi(\alpha)=r>0$，而且对每个 $c\in C$ 有 $\varphi(\alpha-c)\geqslant r$。我们将证明对满足 $\varphi(c)<r$ 的每个复数 c 有 $\varphi(\alpha-c)=r$。为此，令 n 为任意正整数，并考察 $\alpha^n-c^n=(\alpha-c)(\alpha-\varepsilon c)(\alpha-\varepsilon^2 c)\cdots(\alpha-\varepsilon^{n-1}c)$，其中 ε 是一个含于 C 中的 n 次本原单位根。则

$$\begin{aligned}&\varphi(\alpha-c)\varphi(\alpha-\varepsilon c)\cdots\varphi(\alpha-\varepsilon^{n-1}c)\\&\qquad=\varphi(\alpha^n-c^n)\leqslant\varphi(\alpha)^n+\varphi(c)^n.\end{aligned}$$

因为 $\varphi(\alpha-\varepsilon^k c)\geqslant r$，则有

$$\varphi(\alpha-c)r^{n-1}\leqslant\varphi(\alpha)^n\left(1+\frac{\varphi(c)^n}{\varphi(\alpha)^n}\right)=r^n\left(1+\left(\frac{\varphi(c)}{r}\right)^n\right).$$

因此

$$\varphi(\alpha-c)\leqslant r\left(1+\left(\frac{\varphi(c)}{r}\right)^n\right),$$

那么，如果 $\varphi(c)<r$，则由 $\lim\left(1+\left(\frac{\varphi(c)}{r}\right)^n\right)=1$. 得出关系

$\varphi(\alpha-c)=r$。现在我们对满足 $\varphi(c)<r$ 的任意 c，用 $\alpha-c$ 代替 α 得到 $\varphi(\alpha-2c)=r$。如果我们重复这一过程，则对一切 $n=1,2,\cdots$ 和所有使得 $\varphi(c)<r$ 的 c 有 $\varphi(\alpha-nc)=r$。总之，如果 $\varphi(c)<nr$，有 $\varphi(\alpha-c)=r$，又由于 n 是任意的，故对一切 $c\in C$ 有 $\varphi(\alpha-c)=r$。于是若 $c_1,c_2\in C$，则有 $\varphi(c_1-c_2)\leqslant\varphi(\alpha-c_1)+\varphi(\alpha-c_2)=2r$，但由于 φ 等价于 C 上的绝对值赋值，这结果是荒谬的。所以必然有 $C=\Phi$。证毕。

鉴于奥斯特洛夫斯基定理成立，关于一个阿基米得赋值的完备域之赋值扩张定理就显得不大重要了。如果 Φ 关于一个阿基米得赋值是完备的，那么 Φ 或者是实数域或者是复数域。在第一种

情形，仅有的有限维扩张是 Φ 和复数域．在第二种情形，只可能是 Φ．在所有的情形扩张定理均是显然的．如果我们把它和早先的结果综合起来就得到下述的

定理 17. 如果 Φ 关于实赋值 φ 是完备的，P 为 Φ 的有限维扩张，则有且仅有一种方法把此赋值扩张成 P 的赋值．此扩张由公式(38)给出．而且，P 关于它的赋值是完备的．

15. 实赋值在有限维扩张域上的扩张 现在我们处理这样一个问题，它就是要确定一个定义在域 Φ 上的实赋值在一个有限维扩张域 P/Φ 上的一切扩张．对 Φ 是完备域的情形我们在上一节已处理过了．我们将使用已得的结果去处理一般情形的问题．设 $\bar{\Phi}$ 是 Φ 关于 φ 的完备化，并用 $\bar{\varphi}$ 记 φ 在 $\bar{\Phi}$ 中的扩张赋值，现设 (E,s,t) 是 P/Φ 和 $\bar{\Phi}/\Phi$ 的域合成：E 是 Φ 上的一个域，s 和 t 分别是 P/Φ 和 $\bar{\Phi}/\Phi$ 到 E/Φ 内的同构，而 E 是由 P^s 和 $\bar{\Phi}^t$ 生成的域．由于 $[\mathrm{P}:\Phi]=n<\infty$，有 $[E:\bar{\Phi}^t]\leqslant n<\infty$．对 $\bar{\alpha}\in\bar{\Phi}$，定义 $\bar{\varphi}_t(\bar{\alpha}^t)=\bar{\varphi}(\bar{\alpha})$，就可以把 $\bar{\Phi}$ 中的赋值 $\bar{\varphi}$ 转移到 $\bar{\Phi}^t$ 中去．显然 $\bar{\varphi}_t$ 在 Φ 上和 φ 重合．因 $\bar{\Phi}$ 关于 $\bar{\varphi}$ 是完备的，显然 $\bar{\Phi}^t$ 关于 $\bar{\varphi}_t$ 也是完备的．由于 E 是 $\bar{\Phi}^t$ 的有限维扩张，则实赋值 $\bar{\varphi}_t$ 有唯一的 E 上的实赋值扩张 $\bar{\phi}$．设 ϕ_s 是 $\bar{\phi}$ 在子域 P^s 的限制，而且用 $\phi(\rho)=\phi_s(\rho^s)$ 把 ϕ_s 转移至 P，则显然 ϕ 是在 P 上扩张 φ 而得的一个实赋值．

因此，联系到 P 和 $\bar{\Phi}$ 的每个合成 (E,s,t)，我们得到一个把 φ 扩张成 P 上实赋值 ϕ 的过程．我们将证明在合成和赋值的扩张之间的对应是 1—1 的并且是满射的，如果我们把等价的合成看成一样的话．首先，设 P/Φ 和 $\bar{\Phi}/\Phi$ 的两个合成 (E_1,s_1,t_1) 和 (E_2,s_2,t_2) 是等价的，则存在 E_1/Φ 到 E_2/Φ 上的一个同构 u，使得 $\bar{\alpha}^{t_1u}=\bar{\alpha}^{t_2}$，$\bar{\alpha}\in\bar{\Phi}$ 和 $\rho^{s_1u}=\rho^{s_2}$，$\rho\in\mathrm{P}$．对于 $\bar{\Phi}^{t_1}$ 和 $\bar{\Phi}^{t_2}$ 上的赋值，有 $\bar{\varphi}_{t_2}(\bar{\alpha}^{t_2})=\bar{\varphi}(\bar{\alpha})=\bar{\varphi}_{t_1}(\bar{\alpha}^{t_1})$．因此，$\bar{\varphi}_{t_2}(\bar{\alpha}^{t_1u})=\bar{\varphi}_{t_1}(\bar{\alpha}^{t_1})$．设 $\bar{\phi}_1$ 和 $\bar{\phi}_2$ 分别是 E_1 和 E_2 的赋值，它们分别扩张 $\bar{\varphi}_{t_1}$ 和 $\bar{\varphi}_{t_2}$．于是 $\bar{\phi}_2'(\gamma_1^u)=\bar{\phi}_1(\gamma_1)(\gamma_1\in E_1)$ 定义 E_2 上的一个实赋值，使得对于 $\bar{\alpha}^{t_1u}(\in\bar{\Phi}^{t_2})$ 有 $\bar{\phi}_2'(\bar{\alpha}^{t_1u})=\bar{\phi}_1(\bar{\alpha}^{t_1})=\bar{\varphi}_{t_1}(\bar{\alpha}^{t_1})=\bar{\varphi}_{t_2}(\bar{\alpha}^{t_1u})$．所

以 $\bar{\phi}'_2$ 是赋值 φ_{t_2} 在 $\bar{\Phi}'^2$ 上的一个扩张。由于 $\bar{\Phi}'^2$ 是完备的，此扩张是唯一的，故它同 $\bar{\phi}_2$ 重合。因此，有 $\bar{\phi}_1(\gamma_1)=\bar{\phi}_2(\gamma_1^u)$，对每个 $\gamma_1\in E_1$。由此推出限制 ϕ_{s_1} 和 ϕ_{s_2} 到 P^{s_1} 和 P^{s_2} 得 $\phi_{s_1}(\rho^{s_1})=\phi_{s_2}(\rho^{s_1u})=\phi_{s_2}(\rho^{s_2})$。所以，对应在 P 上的赋值 ϕ_1 和 ϕ_2 有 $\phi_1(\rho)=\phi_{s_1}(\rho^{s_1})=\phi_{s_2}(\rho^{s_2})=\phi_2(\rho)$，因此，等价的合成给出了相同的赋值。

反之，对 P 的赋值 ϕ_1,ϕ_2 假定 $\phi_1(\rho)=\phi_2(\rho)$，而它们是由合成 (E_1,s_1,t_1) 和(E_2,s_2,t_2)确定的，那么，有 $\phi_{s_1}(\rho^{s_1})=\phi_{s_2}(\rho^{s_2})$，$\rho\in P$．其次，我们注意到在由 E_i 中的赋值所定义的拓扑中，$E_i(i=1,2)$ 是 P^{s_i} 的闭包．显然，此闭包包含 $\bar{\Phi}^{t_i}$ 和 P^{s_i}，由于E_i是由 $\bar{\Phi}^{t_i}$ 和 P^{s_i} 生成的，从而也包含 E_i。又显然，在定义 5 的意义下 E_i 是 P^{s_i} 关于赋值 ϕ_{s_i} 的完备化．所以由定理 6，P^{s_1} 到 P^{s_2} 上的同构 $\rho^{s_1}\rightarrow\rho^{s_2}$ 能唯一地扩张成 E_1 到 E_2 上的一个等距同构 u，对 E_i 的赋值 ϕ_i 有 $\phi_1(\gamma_1)=\phi_2(\gamma_1^u)$，而且 $\rho^{s_1u}=\rho^{s_2}$。由于 $\bar{\Phi}^{t_i}$ 是Φ在 E_i 中的闭包，u 在Φ上是恒等映射，可见 u 把 $\bar{\Phi}^{t_1}$ 映到 $\bar{\Phi}^{t_2}$ 上．因此，u 在 $\bar{\Phi}^{t_1}$ 上的限制是一个等距同构，且是Φ上的恒等映射．另一方面，由于 $\bar{\varphi}_{t_1}(\bar{\alpha}^{t_1})=\bar{\varphi}(\bar{\alpha})=\bar{\varphi}_{t_2}(\bar{\alpha}^{t_2})$，映射 $\bar{\alpha}^{t_1}\rightarrow\bar{\alpha}^{t_2}$ 有相同的性质．因此，由定理 6，$\bar{\alpha}^{t_1}\rightarrow\bar{\alpha}^{t_2}$ 与映射 u 重合，所以有 $\bar{\alpha}^{t_1u}=\bar{\alpha}^{t_2}$，故 (E_1,s_1,t_1) 和 (E_2,s_2,t_2) 是等价的。

剩下要证明每个关于 P 的、又是φ之扩张的赋值ϕ都能以所指出的方法从一个合成得出．为此，令E是 P 关于ϕ的完备化，用 s 记 P 到E内的一个典范嵌入(同构)，于是就有完备化$\bar{\Phi}$到Φ在E中的闭包内的同构 t。E的由 $\bar{\Phi}^t$ 和 P^s 生成的子域是 $\bar{\Phi}^t$的有限维扩张，故关于从E所得到的赋值是完备的．因而，此子域同E重合．因此，我们有一个合成 (E,s,t)，并可验证从这个合成得到的赋值就是所给定的赋值 ϕ。于是有如下叙述的

定理 18. 设 P 是域Φ的一个有限维扩张域，Φ有实赋值 φ，且设 $\bar{\Phi}$ 是Φ的完备域，则φ扩张为 P 中的赋值ϕ同 P/Φ 和$\bar{\Phi}$之合成 (E,s,t) 的等价类是 1—1 对应的。

在§1.16，我们在合成 (E,s,t) 的等价类和代数 $\bar{\Phi}\otimes_{\Phi}P$ 的极

大理想之间建立了 1—1 对应. 我们看到，如果 $\mathfrak{J}$ 是 $\Phi\otimes P$ 的一个极大理想，那么这就决定了一个合成，其域是 $E=(\Phi\otimes P)/\mathfrak{J}$. 不同的 $\mathfrak{J}$ 给出不等价的合成，而且每个合成都等价于一个从极大理想 $\mathfrak{J}$ 所得到的合成. 我们又看到，极大理想的个数是有限的，而且如果 $\mathfrak{J}_1,\mathfrak{J}_2,\cdots,\mathfrak{J}_h$ 为 $\Phi\otimes P$ 中不同的极大理想，且 $\mathfrak{R}=\bigcap\mathfrak{J}_i$，则 $(\Phi\otimes P)/\mathfrak{R}=E_1\oplus E_2\oplus\cdots\oplus E_h$，其中 $E_i\cong(\Phi\otimes P)/\mathfrak{J}_i$. 域 E_i 是 P 关于一个赋值 ϕ_i 的完备化. 我们将称 $[E_i:\Phi]=n_i$ 为由 ϕ_i 决定的 P 之**局部维数**. 于是我们有

$$
\begin{aligned}
\sum n_i &= [(\Phi\otimes P):\Phi]-[\mathfrak{R}:\Phi] \\
&= [P:\Phi]-[\mathfrak{R}:\Phi] \\
&= n-[\mathfrak{R}:\Phi]\leqslant n.
\end{aligned}
\tag{41}
$$

而且，$\sum n_i=n$ 当且仅当 $\mathfrak{R}=0$. 由于可把 $\Phi\otimes P$ 看成 Φ 上的有限维代数，由导言的 VII 得出，$(\Phi\otimes P)/\mathfrak{J}$ 是一个域当且仅当它是一个整区. 因此，$\mathfrak{J}$ 在 $(\Phi\otimes P)$ 内是极大理想当且仅当 $\mathfrak{J}$ 是素理想. 所以，由定理 12，$\bigcap\mathfrak{J}_i=\mathfrak{R}$ 是代数 $\Phi\otimes P$ 的根，即是说，$\mathfrak{R}$ 是 $\Phi\otimes P$ 之幂零元的集，而且 $\mathfrak{R}=0$ 当且仅当 $\Phi\otimes P$ 没有非零幂零元. 如果 P 在 Φ 上是可分的，则 $\Phi\otimes_\Phi P=E_1\oplus E_2\oplus\cdots\oplus E_h$，其中 E_i/Φ 是域，它是由 P 关于 Φ 之本原元 θ 的最小多项式所决定的(§1.16). 由于域的直和不包含非零幂零元，那么显然有：如果 P 关于 Φ 是可分的，则 $\Phi\otimes P$ 有零根 $\mathfrak{R}$，所以，在此情况下，公式(41)变为

$$
n=\sum n_i. \tag{42}
$$

习　题　44

1. 对 $p=3,5,11$，决定有理数域的 p-adic 赋值在五次单位根的分圆域上扩张的个数.

16. 分歧指数与剩余次数　设 Φ 是域，具有非平凡非阿基米得实赋值 φ，并设 γ 是赋值群，$\mathfrak{o}/\mathfrak{p}$ 是 Φ 关于 φ 的剩余域(§5). 设 P 是有限维扩张域，ϕ 是赋值 φ 在 P 上的一个扩张，Γ 是对应的赋值群，$\mathfrak{O}/\mathfrak{P}$ 是 P 的剩余域. 由于 $\mathfrak{O}$ 和 $\mathfrak{P}$ 分别是满足 $\phi(\rho)\leqslant 1$，

$\phi(\rho)<1$ 的元之集，显然有 $\mathfrak{o}\leqslant\mathfrak{O}$ 和 $\mathfrak{p}=\mathfrak{o}\cap\mathfrak{P}$. 因此，我们可以把剩余域 $\mathfrak{o}/\mathfrak{p}$ 和剩余域 $\mathfrak{O}/\mathfrak{P}$ 的子域 $(\mathfrak{o}+\mathfrak{P})/\mathfrak{P}$ 等同起来. 据此，可以考虑维数 $[\mathfrak{O}/\mathfrak{P}:\mathfrak{o}/\mathfrak{p}]=f$，我们将称这个维数为扩张 P/Φ 之赋值 ϕ 的**剩余次数**. 显然，值群 γ 是 Γ 的子群，并称 γ 在 Γ 中的指数 e 为 ϕ 的**分歧指数**. 如果 $\rho\in P$，则我们可以用 P 的一个适当的非零元乘 ρ 得到 $\mathfrak{P}$ 的一个元. 所以，我们可以取 $\mathfrak{P}$ 的一个元作为 γ 在 Γ 中陪集的代表. 剩余次数和分歧指数两者均是有限的. 事实上，有

引理 1. $ef\leqslant n=[P:\Phi]$.

证 设 $\rho_1,\rho_2,\cdots,\rho_{f_1}$ 是 $\mathfrak{O}$ 的元，它们在 $(\mathfrak{o}+\mathfrak{P})/\mathfrak{P}$ 上线性无关. 那么，如果 α_i 是 $\mathfrak{o}$ 的元，而且 $\sum\alpha_i\rho_i\in\mathfrak{P}$，则每个 $\alpha_i\in\mathfrak{p}$. 设 $\pi_1,\pi_2,\cdots,\pi_{e_1}$ 是 $\mathfrak{P}$ 的元使得陪集 $\phi(\pi_1)\gamma,\ \cdots,\phi(\pi_{e_1})\gamma$ 在 Γ/γ 中是不同的. 我们可断言这 e_1f_1 个元 $\rho_i\pi_j$ 是 Φ 无关的. 设 $\sum\alpha_{ij}\rho_i\pi_j=0$，其中 $\alpha_{ij}\in\Phi$. 首先，我们要证明，如果 $\alpha_i\in\Phi$ 且 $\sum\alpha_i\rho_i\neq0$，则 $\phi(\sum\alpha_i\rho_i)\in\gamma$. 如果 $\sum\alpha_i\rho_i\neq0$，则某些 $\alpha_i\neq0$，我们可假定 $0\neq\phi(\alpha_1)\geqslant\phi(\alpha_i)$. 于是，如果 $\beta_i=\alpha_i\alpha_1^{-1}$，就有 $\phi(\beta_i)\leqslant1$，那么 β_i 属于 φ 的赋值环 $\mathfrak{o}$. 我们有 $\sum\alpha_i\beta_i=\alpha_1(\sum\beta_i\rho_i)$. 又有 $\phi(\sum\beta_i\rho_i)\leqslant1$，由于 $\beta_1=1$ 和 $\beta_i\in\mathfrak{o}$，显然 $\phi(\sum\beta_i\rho_i)<1$ 将和 ρ_i 在 $\mathfrak{o}+\mathfrak{P}/\mathfrak{P}$ 上的线性无关性矛盾. 因此，可得 $\phi(\sum\beta_i\rho_i)=1$，那么 $\phi(\sum\alpha_i\rho_i)=\phi(\alpha_1)(\phi(\sum\beta_i\rho_i))=\phi(\alpha_1)\in\gamma$. 现在，我们回过头来看看关系式 $\sum\alpha_{ij}\rho_i\pi_j=0$，$\alpha_{ij}\in\Phi$. 设存在一个 i 使得 $\phi(\sum\alpha_{ij}\rho_i)\neq0$，则存在不同的 j，譬如 $j=1,2$，使得 $\phi(\sum\alpha_{i1}\rho_i\pi_1)=\phi(\sum\alpha_{i2}\rho_i\pi_2)\neq0$（§1，习题的第 2 题）. 那么 $\phi(\sum\alpha_{i1}\rho_i)\ \phi(\pi_1)=\phi(\sum\alpha_{i2}\rho_i)\ \phi(\pi_2)\neq0$，而由已经证明的结果可得 $\gamma\phi(\pi_1)=\gamma\phi(\pi_2)$. 这和 π 的选法矛盾. 因此对每个 j，必须有 $\phi(\sum\alpha_{ij}\rho_i)=0$ 或者 $\sum\alpha_{ij}\rho_i=0$. 重复前面曾用过的推理，基于 ρ_i 在 $(\mathfrak{o}+\mathfrak{P})/\mathfrak{P}$ 上的线性无关性可得每个 $\alpha_{ij}=0$. 这就证明了我们的断言：这 e_1f_1 个元 $\rho_i\pi_j$ 是 Φ 无关的. 因此 $e_1f_1\leqslant n$. 显然，由 e_1 和 f_1 的定义可得 $ef\leqslant n$.

引理 2. 如果 φ 是离散的而且 Φ 关于 φ 是完备的，则 $ef=$

n.

证. 由于φ是离散的,故赋值ϕ在P内也是离散的,而且P是完备的. 群γ和Γ是循环的, 而 Γ/γ 是e阶循环群. 设π和β分别是 $\mathfrak{P}$ 和 $\mathfrak{p}$ 的使 $\phi(\pi)$ 和 $\phi(\beta)=\varphi(\beta)$ 为极大的元. P的任何非零元有形式 $\varepsilon\pi^k$,其中 $\phi(\varepsilon)=1$,而 $k=0,\pm1,\pm2,\cdots$. 因此 $\phi(\pi)$ 是Γ的一个生成元. 如果 $\beta=\eta\pi^{e'}$,其中 $\phi(\eta)=1$,而且由于 $\beta\in\mathfrak{p}\subseteq\mathfrak{P}$ 有 $e'>0$,那么 $\phi(\pi)^{e'}\in\gamma$,故e'可以被陪集$\phi(\pi)\gamma$ 的阶e整除. 另一方面,$\phi(\pi)^e=\phi(\pi^e)=\phi(\beta')$, 对某些$\beta'\in\mathfrak{P}$,而且 $\beta'=\zeta\beta^k$,其中 $\phi(\zeta)=1$. 因此,$\phi(\pi^e)=\phi(\beta^k)=\phi((\eta\pi^{e'})^k)=\phi(\pi^{e'k})$. 故 $e=e'k$. 由此得 $k=1,e'=e$, 于是有关系式 $\beta=\eta\pi^e,\phi(\eta)=1$,而$e$是 Γ/γ 的阶. 设 $\rho_1,\rho_2,\cdots,\rho_f$ 是 $\mathfrak{O}$ 的元,使得陪集 $\rho_i+\mathfrak{P}$ 组成域 $\mathfrak{O}/\mathfrak{P}$ 关于子域$(\mathfrak{o}+\mathfrak{P})/\mathfrak{P}\cong\mathfrak{o}/\mathfrak{p}$ 的一个基. 我们将证明元 $\rho_i\pi^j,1\leqslant i\leqslant f,0\leqslant j\leqslant e-1$ 组成P关于Φ的一个基. 由于 $\phi(\pi)\gamma$ 的阶为 e, $\phi(1),\phi(\pi),\cdots,\phi(\pi^{e-1})$落在关于$\gamma$的不同的陪集中; 故由引理1的证明可知元 $\rho_i\pi^j$ 是Φ无关的. 剩下要证明P的每个元是这些元的Φ线性组合;首先要证明 $\mathfrak{O}$ 的每个元是系数取自 $\mathfrak{o}$中的元 $\rho_i\pi^j$ 的线性组合: 设 $\nu\in\mathfrak{O}$. 则对某些 $k\geqslant0$有 $\phi(\nu)=\phi(\pi^k)$. 可记$k=m_1e+j_1$,其中 $m_1\geqslant0$, $0\leqslant j_1\leqslant e-1$. 则 $\phi(\nu)=\phi(\beta^{m_1}\pi^{j_1})$, 故 $\mu=(\beta^{m_1}\pi^{j_1})^{-1}\nu$ 满足$\phi(\mu)=1$. ρ_i 的定义表明存在元$\alpha_{1i}\in\mathfrak{o}$使得 $\mu-\sum_1^f\alpha_{1i}\rho_i\in\mathfrak{P}$. 于是 $\phi(\sum\alpha_{1i}\rho_i)=\phi(\mu)=1$, 而且如果 $\nu_1=\beta^{m_1}\pi^{j_1}(\mu-\sum\alpha_{1i}\rho_i)$,则 $\phi(\nu_1)<\phi(\nu)$. 我们有

$$\nu=\beta^{m_1}\pi^{j_1}\mu=\beta^{m_1}\pi^{j_1}(\sum\alpha_{1i}\rho_i)+\nu_1. \tag{43}$$

对 ν_1 重复上述的论证并得到序列 $\nu_1,\nu_2,\cdots$,使得

$$\nu_{k-1}=\beta^{m_k}\pi^{j_k}(\sum\alpha_{ki}\rho_i)+\nu_k, \tag{44}$$

其中 $\alpha_{ki}\in\mathfrak{o},m_k\geqslant0,0\leqslant j_k\leqslant e-1,\phi(\sum\alpha_{ki}\rho_i)=1$ 而且 $\phi(\nu_k)<\phi(\nu_{k-1})$. 由(44) 可得 $\phi(\nu_{k-1})=\phi(\beta^{m_k}\pi^{j_k})$. 于是 $\nu_k\to0$, $\beta^{m_k}\to0,(\sum\alpha_{ki}\rho_i)\beta^{m_k}\to0$. 由最后一个极限推出, 如果无穷级数的项作成序列 $(\sum\alpha_{ki}\rho_i)\beta^{m_k}(k=1,2,\cdots)$ 的子序列则此无穷级

数收敛。由(43)和(44)得

$$(45)\qquad \nu = \beta^{m_1}\pi^{j_1}(\sum \alpha_{1i}\rho_i) + \beta^{m_2}\pi^{j_2}(\sum \alpha_{2i}\rho_i) + \cdots + \beta^{m_k}\pi^{j_k}(\sum \alpha_{ki}\rho_i) + \nu_k.$$

由于 $\nu_k \to 0$ 和 (45)中各个幂 $\pi^j(0 \leqslant j \leqslant e-1)$ 的系数收敛，故由(45)得 $\nu = \sum \beta_{ij}\rho_i\pi^j$，$0 \leqslant j \leqslant e-1$，其中 $\beta_{ij} \in \mathfrak{o}$. 现在令 ν 是 P 的任一个元，则可找一个 β 的幂使得 $\nu\beta^{-k} \in \mathfrak{O}$. 故得 $\nu = \beta^k(\sum \beta_{ij}\rho_i\pi^j)$，其中 $\beta_{ij} \in \mathfrak{o}$，那么 P 的每个元是 $\rho_i\pi^j$ 的 Φ 线性组合。

现可证明

定理 19. 设 Φ 是一个具有非阿基米得实赋值[1]的域，P 是 Φ 的一个有限维扩张域，$\phi_1, \phi_2, \cdots, \phi_k$ 是扩张 φ 的 P 的不同赋值，并设 e_i, f_i 分别为 P/Φ 关于 ϕ_i 的分歧指数和剩余次数，则

$$(46)\qquad \sum_{i}^{h} e_i f_i \leqslant n = [P:\Phi],$$

而且如果 P 在 Φ 上是可分的和 φ 是离散的，则

$$(47)\qquad \sum_{1}^{h} e_i f_i = n$$

成立。

证. 设 E_i 是 P 关于 ϕ_i 的完备化，则对 Φ 的完备化 $\bar{\Phi}$ 和 $n_i = [E_i:\bar{\Phi}]$ 有 $\sum n_i \leqslant n$，而且因为 P 在 Φ 上是可分的故有 $\sum n_i = n$. 在 §5 我们曾证明过 E_i 和 P 关于 ϕ_i 有相同的值群，而且 $\bar{\Phi}$ 和 Φ 关于 φ 有相同的值群. 因此 P 在 Φ 上关于 ϕ_i 的分歧指数与 E_i 在 $\bar{\Phi}$ 上的相同. 类似地，§5 和定义表明 P/Φ 关于 ϕ_i 的剩余次数 f_i 与 $E/\bar{\Phi}$ 的相同. 由引理 1 和 2，我们有 $e_i f_i \leqslant n_i$，若此赋值还是离散的，则 $e_i f_i = n_i$. 因此，总有 $\sum e_i f_i \leqslant \sum n_i \leqslant n$，如果 P/Φ 是可分的，φ 是离散的，则 $\sum e_i f_i = \sum n_i = n$.

习 题 45

1. 在 §15，习题的第 1 题的情况下，决定剩余次数和分歧指数。

---

1) 应为"实赋值 φ"——译者注.

第 六 章

阿廷-施莱尔（Artin-Schreier）理论

在这一章我们将考虑由阿廷和施莱尔建立的形式实域理论．实数域的基本代数性质是在此域中关系式 $\sum\alpha_i^2=0$ 仅在平凡的情形才能成立：$0^2+0^2+\cdots+0^2=0$．这种观察引导阿廷和施莱尔称具有此性质的任意域为形式实域．任何这样的域都可以有序化，另一方面，任一有序域都是形式实域．在此理论中，我们最感兴趣的是实闭域，它在代数扩张的意义下是极大的形式实域．一个实闭域有唯一的序，此序可用下列条件来刻划：在这样的域中，$\alpha>0$，当且仅当 $\alpha=\beta^2\neq 0$．还有，如果 P 是实闭的，则$P(\sqrt{-1})$是代数封闭的．任何形式实域都能嵌入一个实闭域，而此域在给定的域上是代数的．而且，如果原来的域是有序的，那么还可以这样来嵌入，使得在实闭代数扩张中的那个唯一的序是给定域的序的扩张．这样一个有序域的实闭扩张本质上是唯一的，并称为有序域的实闭包．

阿廷-施莱尔理论的典型应用是确定一个域的哪些元可表示为此域中元的平方和问题．对有理数的有限代数扩张，此问题有一个由希尔伯特和兰道（Landau）给出的简单的回答（定理 11）．形式实域的理论促使阿廷解决关于正定有理函数分解为平方和的希尔伯特问题．我们将给出阿廷定理的证明(定理 12)．

继阿廷和施莱尔原来工作之后，形式实域理论的最重要的发展是塔尔斯基的元数学原理，此原理断言任一个代数的初等命题如果对一个实闭域成立则对每个实闭域也成立．这一原理基于一个算法，这个算法用于判别在一个实闭域中有限组有理系数的多项式方程与不等式的可解性．最初塔尔斯基给出了一个判别法．

我们将给出另一个属于赛登堡的判别法.

在最后一节,我们要建立实闭域的阿廷-施莱尔刻划,即它不是代数闭域,而是代数闭域中的一个有有限余维数的域.

1. 有序域与形式实域 在上一章我们定义过有序群(§5.7).用类似的方法,我们有下述的

定义 1. 有序域Φ是一个域Φ连同Φ的一个子集 P(正元的集),使得:(1) $0 \notin P$,(2)如果 $\alpha \in \Phi$,则或者 $\alpha \in P$,或者 $\alpha = 0$,或者$-\alpha \in P$,(3) P 对加法和乘法是封闭的.

由于任一个域不止包含一个元,显然子集 P 非空.如果用N记集 $\{-\alpha | \alpha \in P\}$,则(2)断言 $\Phi = P \cup \{0\} \cup N$.而且,由(1)显然有 $P \cap \{0\} = \varnothing, N \cap \{0\} = \varnothing$,因为如果 $\alpha \in P \cap N$,则$-\alpha \in P \cap N$,于是 $0 = \alpha + (-\alpha) \in P$,这与(1)矛盾,故 $P \cap N = \varnothing$.因此,分解式 $\Phi = P \cup \{0\} \cup N$ 是不相交之集的并.显然N对加法是封闭的,因为如果 $\alpha, \beta \in P$,则 $(-\alpha) + (-\beta) = -(\alpha + \beta) \in N$.另方面,如果$-\alpha, -\beta \in N$,则 $(-\alpha)(-\beta) = \alpha\beta \in P$.

如果 $\alpha - \beta \in P$,定义 $\alpha > \beta$,这样就可以在有序域Φ(更确切地说是 Φ,P)中引进一个偏序. 如果α, β 是Φ的任意两个元,我们有三歧性:关系 $\alpha > \beta, \alpha = \beta, \beta > \alpha$ 有且仅有一种成立.因此,按关系 $\alpha > \beta$, Φ有线性序. 如果 $\alpha > \beta$,则 $\alpha + \gamma > \beta + \gamma$,而且若 $\delta > 0$,还有 $\alpha\delta > \beta\delta$.反之,如果有一个线性序$>$,它使得由$\alpha > \beta$ 推出 $\alpha + \gamma > \beta + \gamma$ 和由 $\delta > 0$ 推出 $\alpha\delta > \beta\delta$.我们就可以利用这样的线性序定义一个有序域.用 P 表示 $\alpha > 0$ 的元之集,可直接推得 Φ, P 在原来的意义F是一个有序域,而且由 Φ, P 定义的关系 $>$ 是给定的序关系.

通常把$\beta > \alpha$ 记为$\alpha < \beta$ 是方便的.在实数域中序的初等性质是容易建立的.我们列出其中一些性质:由 $\alpha > 0$ 得出 $\alpha^{-1} > 0$,而且由 $\alpha > \beta > 0$ 推出 $\beta^{-1} > \alpha^{-1} > 0$.如果 $\alpha > \beta$,则$-\alpha < -\beta$ 而且,如果 $\alpha > \beta, \gamma > \delta$,则 $\alpha + \gamma > \beta + \delta$.与通常一样,定义$|\alpha| = \alpha$,如果 $\alpha \geqslant 0$;$|\alpha| = -\alpha$,如果 $\alpha < 0$,而且能证明 $|\alpha + \beta| \leqslant |\alpha| + |\beta|, |\alpha\beta| = |\alpha||\beta|$.

如果 Φ' 是有序域 Φ, P 的子域,则 Φ' 关于 $P' = \Phi' \cap P$ 是有序的. 我们称这个序为 Φ' 中的导出序. 显然,在 Φ', P' 中, $\alpha' > \beta'$ 当且仅当在 Φ, P 中 $\alpha' > \beta'$. 如果 Φ, P 和 Φ', P' 是任两个有序域,则 Φ 到 Φ' 内的同构 s 称为序同构(或者有序域的同构),如果 $P^s \subseteq P'$. 由此得 $N^s \subseteq N'$, N' 为 P' 的元之负元集,而且如果 s 是满射的,则 $P^s = P'$, $N^s = N'$.

在任一个有序域 Φ 中,由 $\alpha \neq 0$ 可得 $\alpha^2 > 0$. 因此,如果 α_1, $\alpha_2, \cdots, \alpha_r \neq 0$,则 $\sum \alpha_i^2 > 0$. 这就证明了在下述的意义下任何有序域是形式实域:

定义 2. 一个域 Φ 是形式实域,如果在 Φ 中,关系式 $\sum_{i=1}^{r} \alpha_i^2 = 0$ 仅当每个 $\alpha_i = 0$.

可直接推得, Φ 是形式实域当且仅当 -1 不是 Φ 的元的平方和. 如果 Φ 的特征 $p \neq 0$, 则 $0 = 1^2 + 1^2 + \cdots + 1^2$ (p 项);因此,形式实域的特征必须为 0.

在任何域中, 令 $\sum(\Phi)$ 记 Φ 中能表为平方和的元之子集.显然 $\sum(\Phi)$ 包含 0, 并且对加法和乘法是封闭的. 而且, 已知 Φ 是形式实域当且仅当 $-1 \notin \sum(\Phi)$. 如果在 $\sum(\Phi)$ 内 $\beta \neq 0$, 则 $\beta^{-1} \in \sum(\Phi)$;因为若 $\beta = \sum \beta_i^2$, 那么, $\beta^{-1} = \beta(\beta^{-1})^2 = \sum(\beta_i \beta^{-1})^2$. 我们也注意到,如果 Φ 不是形式实域而且特征不为 2,则 $\sum(\Phi) = \Phi$;因为 $-1 \in \sum(\Phi)$; 因为 $-1 \in \sum(\Phi)$ 且若 α 是 Φ 的任一元, 则

$$\alpha = \left(\frac{1+\alpha}{2}\right)^2 - \left(\frac{1-\alpha}{2}\right)^2 = \left(\frac{1+\alpha}{2}\right)^2 + (-1)\left(\frac{1-\alpha}{2}\right)^2$$

$\in \sum(\Phi)$,这是因为 $\sum(\Phi)$ 对加法和乘法是封闭的. 将关于 $\sum(\Phi)$ 的这些结果叙述成如下引理会是有用的

引理. 设 Φ 是一个域, $\sum(\Phi)$ 是 Φ 中能表为平方和的元之子集, 则 $\sum(\Phi)$ 对加法和乘法是封闭的, 且对 $\sum(\Phi)$ 中的每个 $\beta \neq 0$ 有 $\beta^{-1} \in \sum(\Phi)$. 如果 Φ 不是形式实域且特征不为 2, 则 $\sum(\Phi) = \Phi$.

习 题 46

1. 证明有理数域有且仅有一种方法序化.

2. 证明如果 R_0 为有理数域,则域 $R_0(\sqrt{2})$ 恰有两种不同的序.

3. 设 Φ 是一个有序域, $f(x)=x^n+\alpha_1x^{n-1}+\cdots+\alpha_n$ 是一个系数在 Φ 中的多项式, $M=\max(1,|\alpha_1|+|\alpha_2|+\cdots+|\alpha_n|)$, 证明 $f(x)$ 在 Φ 中的每个根含于区间 $-M\leqslant x\leqslant M$.

4. 证明形式实域的任意纯超越扩张是形式实域.

5. 设 R_0 为有理数域, $\Phi=R_0(\xi)$, 而 ξ 为超越元, 证明 Φ 有不可数个不同的序.

6. 设 Φ 是形式实域, $\mathfrak{H}(\Phi_n)$ 表示 $n\times n$ 阶对称矩阵集, 其元在 Φ 内. 证明 $\mathfrak{H}(\Phi_n)$ 在下述意义下是形式实的: 由 $\sum A_i^2=0$, $A_i\in\mathfrak{H}(\Phi_n)$, 可推得每个 $A_i=0$.

7. 设 (x,y) 是 Φ 上 n 维向量空间 $\mathfrak{M}$ 上的对称双线性型, 而 Φ 是一个有序域. 设 $\{\beta_1,\beta_2,\cdots,\beta_n\}$ 对 (x,y) 为一个对角阵. 证明下述西尔维斯特定理(卷 2. 中译本, p. 139) 的推广: 正元 β_i 的个数是 (x,y) 的一个不变量.

8. 一个有序域称为阿基米得的,如果给定任意 $\alpha>0,\beta>0$,则存在整数 n 使得 $n\alpha>\beta$ (等价于: 给定 $\alpha>0$, 则存在整数 n 使得 $n>\alpha$). 设 P 是一个有序域, Φ 为有导出序的一个子域, 证明 P 是阿基米得的, 如果: 1) Φ 是阿基米得的, 2) $[\mathrm{P}:\Phi]<\infty$. (提示: 利用第 3 题.)

9. 证明任一阿基米得有序域序同构于实数域 R 的一个子域(参看定理 5.b).

10. (柯恩 (Cohn)). 设 Φ 为以 P 为正元集的有序域,证明 $\Phi(\xi)$ (ξ 为 Φ 上的超越元)能作为有序域, 如果这样选取 P_ξ 作为正元集: 它包含形如 $\beta\xi^r fg^{-1}$ 的元, 其中 $\beta\in\mathrm{P}$, f 和 g 是常数项为 1 的 ξ 的多项式. 证明 $\Phi(\xi)$ 不是阿基米得有序域.

11. (柯西). 设 Φ 是有序域, ξ,η 为 $\Phi(\xi,\eta)$ 中关于 Φ 的代数无关元, 如第 10 题一样序化 $\Phi(\xi)$, 然后把 $\Phi(\xi,\eta)$ 看作 $\Phi(\xi)$ 上的纯超越扩张, 对 $\Phi(\xi,\eta)$ 重复此过程. 证明 $\Phi(\xi,\eta)$ 的每个元必能被 $\Phi(\eta)$ 的一个元所超过, 但在 ξ 和 ξ^2 之间不存在 $\Phi(\eta)$ 的元.

12. 设 P 是一个有序域, Φ 是一个子域. 设 $\mathfrak{p}$ 是 P 的元 β 的集, 并满足: 对 Φ 中每个 $\alpha\neq0$, 有 $|\beta|<|\alpha|$. 并设 $\mathfrak{o}=\{\gamma\in\mathrm{P}\mid\gamma\mathfrak{p}\subset\mathfrak{p}\}$. 证明 $\mathfrak{o}$ 是 P 中含 Φ 的赋值环, 而且 $\mathfrak{p}$ 是 $\mathfrak{o}$ 的非单位的理想. 证明剩余域 $\mathfrak{o}/\mathfrak{p}$ 能如下被序化: 如果 $\gamma\notin\mathfrak{p}$ 且在 P 中 $\gamma>0$, 定义 $\gamma+\mathfrak{p}>0$. 证明 $\mathfrak{o}/\mathfrak{p}$ 是 Φ 的一个扩张(把 Φ 与 $(\Phi+\mathfrak{p})/\mathfrak{p}$ 等同起来), 而且在如下意义下它是 Φ 的一个阿基米得扩张: 每个区间 (a,b) ($a,b\in\mathfrak{o}/\mathfrak{p}$) 都包含 Φ 的一个元.

2. 实闭域 形式实域的深刻性质与如下定义的实闭域有关:

定义 3. 一个域 Φ 称为实闭的,如果 Φ 是形式实域, 但 Φ 的任何真代数扩张都不是形式实域.

我们首先证明任何实闭域有且仅有一种方法被序化, 这是下述定理的一个简单推论.

定理 1. 如果Φ是实闭的，则Φ的任何元或者是一个平方或者是一个平方的负元.

证　设α是Φ的一个非平方的元，则我们能构作真代数扩张$\Omega=\Phi(\sqrt{\alpha})$. 此域不是形式实域，那么在$\Phi$中存在不全为0的$\beta_i,\gamma_i$使得$\sum(\beta_i+\gamma_i\sqrt{\alpha})^2=0$,故$\sum(\beta_i^2+\gamma_i^2\alpha)+2(\sum\beta_i\gamma_i)\sqrt{\alpha}=0$. 因为$\sqrt{\alpha}\notin\Phi$,故$2\sum\beta_i\gamma_i=0$和$\sum\beta_i^2+2\sum\gamma_i^2=0$. 由于$\Phi$是形式实域,$\sum\gamma_i^2\neq0$,故$-\alpha=(\sum\beta_i^2)(\sum\gamma_i^2)^{-1}$.应用§1中引理所叙述的平方和的集$\sum(\Phi)$的性质得到$-\alpha\in\sum(\Phi)$. 由于$\Phi$是形式实域有$-1\notin\sum(\Phi)$，故得$\alpha\notin\sum(\Phi)$. 因此证明了：如果$\Phi$的一个元不是一个平方,则它就不是一个平方和. 换句话说,如果$\alpha\in\sum(\Phi)$则α是一个平方. 而且我们知道，如果α不是一个平方,则$-\alpha\in\sum(\Phi)$,于是由此得$-\alpha$是一个平方. 证毕.

现在我们可以证明

定理 2. 任一实闭域都有且仅有一种方法被序化. 此域的任一自同构都是序同构.

证　设P为实闭域Φ的各非零平方元的子集，则$0\notin P$而且如果$\alpha\neq0$和$\alpha\notin P$,由定理1得$-\alpha\in P$. 如果$\alpha=\beta^2$和$\gamma=\delta^2\in P$，则$\alpha+\gamma\in P$. 否则$\alpha+\gamma=-\varepsilon^2$，$\varepsilon\in P$. 故$\beta^2+\delta^2+\varepsilon^2=0$，这与$\Phi$的形式实域性矛盾. 因此子集P满足有序域的条件1,2,3,即Φ, P是有序域. 设P′是Φ的任一子集,它给出Φ的一个序. 如果$\alpha\in P,\alpha=\beta^2\neq0$,则在P′给出的序中$\alpha>0$，因此$P'\supseteq P$. 由此得$P'=P$,故$\Phi$中的序是唯一确定的. 若$s$是$\Phi$的一个自同构,则$s$显然把非零平方元的集P′映入自身. 因此$s$是$\Phi$的一个序同构.

实闭域存在的问题是非常容易解决的. 事实上，我们有下述的

定理 3. 设Φ是形式实域,Ω是Φ的代数闭包,则Ω包含一个含Φ的实闭域.

证. 考察Ω内含Φ的形式实子域的集族. 由于含有Φ，故此集族非空. 而且此集族是归纳的，那么由佐伦引理得它含有一个

极大元Δ. 如果Δ不是实闭的,则它有一个真代数扩张Δ'是形式实域. 因为Ω是代数封闭的, 故可设 $\Delta'\subseteq\Omega$ (§4.1, 习题的第1题). 这与Δ在Ω内的极大性矛盾,故Δ是实闭的.

显然由定理2和定理3以及任意域的代数闭包的存在性可得下述推论.

推论 1. 可以把任一形式实域嵌入一个实闭域中, 而此域在给定的域上是代数的.

推论 2. 任一形式实域均可序化.

如果Φ是实闭的, 则-1在Φ中不是一个平方元, 那么$\Phi(\sqrt{-1})\supset\Phi$. 我们将证明$\Phi(\sqrt{-1})$是代数封闭的, 并将发现此性质是实闭域的特征. 为此我们首先证明下述的结果.

定理 4. 如果Φ是实闭的, 则系数在Φ内的每个奇次多项式在Φ内有一个根.

证 对次数为1的多项式定理显然成立. 对$f(x)$的次数n用归纳法: 如果$f(x)$是可约的, 则有一个因式[1]是奇数次的, 那么$f(x)$在Φ内有一个根. 因此可以设$f(x)$是不可约的. 设$\Delta=\Phi(\theta)$, 而$f(\theta)=0$, 则$\Delta\supset\Phi$, 于是Δ不是形式实域. 因此有关系式$\sum\varphi_i(\theta)^2=-1$, 其中$\varphi_i(x)$是次数$\leqslant n-1$的$x$的多项式. 由此关系式推得$\sum\varphi_i(x)^2=-1+f(x)g(x)$. $\sum\varphi_i(x)^2$的首项系数对于Φ的序来说是正的,而此多项式的次数是偶数且$\leqslant 2(n-1)$. 由此得$\deg f(x)$是奇数且$\leqslant 2(n-1)-n=n-2$. 因此存在$\beta\in\Phi$使得$g(\beta)=0$. 把β代入关系式$\sum\varphi_i(x)^2=-1+f(x)g(x)$得$\sum\varphi_i(\beta)^2=-1$,但这与$\Phi$的形式实性矛盾. 证毕.

下面我们把所谓的代数基本定理推广到实闭域去. 此证明几乎完全仿照高斯(Gauss)对于这个古典结果的证明.

定理 5. 设Φ是一个有序域,使得: (1)Φ内的正元在Φ内有平方根,(2)任一个系数在Φ内的奇次多项式在Φ中有一个根. 则$\sqrt{-1}\notin\Phi$, $\Phi(\sqrt{-1})$是代数闭合的.

---

1) 指真因式——译者注.

证. 由于Φ是实的,显然有$\sqrt{-1}\notin\Phi$.考虑$\Phi(\sqrt{-1})\supset\Phi$. 令$\rho\to\bar{\rho}$是$\Phi(\sqrt{-1})$在$\Phi$上的自同构使得$\bar{i}=-i$,其中$i=\sqrt{-1}$. 如果$f(x)\in\Phi(\sqrt{-1})[x]$, 则$f(x)\bar{f}(x)\in\Phi[x]$,而且如果此多项式在$\Phi(\sqrt{-1})$中有一个根,则$f(x)$在$\Phi(\sqrt{-1})$中有一个根.因此,如果能证明系数在$\Phi$中的每个非常数多项式在$\Phi(\sqrt{-1})$中有根,就可以得到$\Phi(\sqrt{-1})$是代数闭的. 利用(2), 如果此多项式是奇数的话,则此结论是成立的. 下面我们证明$\Phi(\sqrt{-1})$的每个元在此域中有一个平方根:首先,如果$\alpha\in\Phi,\alpha>0$,则由(1), $\alpha=\beta^2$, $\beta\in\Phi$. 其次, 如果$\alpha\in\Phi$且$\alpha<0$, 则$-\alpha=\beta^2$, $\alpha=(\sqrt{-1})^2\beta^2$. 现令$\rho=\alpha+\beta i$, $i=\sqrt{-1}$,$\alpha,\beta\in\Phi$, $\beta\neq0$. 考虑元$\xi+\eta i$, ξ, $\eta\in\Phi$. 可得$(\xi+\eta i)^2=\xi^2-\eta^2+2\xi\eta i$, 那么$(\xi+\eta i)^2=\alpha+\beta i$ 等价于

(1) $$\xi^2-\eta^2=\alpha,\quad 2\xi\eta=\beta.$$

由于$\beta\neq0$,可以设(用Φ的适当元乘之即得)$\beta=2$, 那么,第二个方程就变为$\xi\eta=1$.如果$\eta=\xi^{-1}$,则此式成立.从而第一个方程变为$\xi^2-\xi^{-2}=\alpha$, 或者$\lambda-\lambda^{-1}=\alpha(\lambda=\xi^2)$. 由于$\alpha^2+4>0$,故方程$\lambda^2-\alpha\lambda-1=0$在$\Phi$中有解$(\alpha+\sqrt{\alpha^2+4})/2$. 因$\alpha+\sqrt{\alpha^2+4}>0$(否则由$\alpha+\sqrt{\alpha^2+4}\leqslant0$将导致$4\leqslant0$), 故$\Phi$中存在一个$\xi\neq0$,使得$\xi^2=\dfrac{1}{2}(\alpha+\sqrt{\alpha^2+4})$. 故$\xi^4-\alpha\xi^2=1$,$\xi^2-\xi^{-2}=\alpha$. 所以$\xi$和$\eta=\xi^{-1}$满足$\beta=2$时的式(1). 至此我们证明了$\Phi(\sqrt{-1})$的每个元在此域中有平方根. 所以不存在$\Phi(\sqrt{-1})$的扩张域$\Delta$使得

$$[\Delta:\Phi(\sqrt{-1})]=2.$$

我们再利用这一事实去证明系数在Φ中的每个正次数多项式在$\Phi(\sqrt{-1})$中有根. 设$f(x)$是这样一个多项式,E是Φ上的$(x^2+1)f(x)$的分裂域. 不妨设$E\supseteq\Phi(\sqrt{-1})$. 因为特征是0,$E$是$\Phi$上的伽罗瓦域. 设$G$是它的伽罗瓦群,$(G:1)=2^em$,而$m$是奇数. 由西洛(*Sylow*)定理,$G$有$2^e$阶的子群$H$. 设$\Delta$是$\Phi$上的$H$不变的子域,则$[E:\Delta]=2^e$,$[\Delta:\Phi]=m$. 因为$\Phi$没有奇数

维真扩张域，必有 $\Delta=\Phi, m=1$. 因此，$G=H$ 且有阶 2^e. 这样的群是可解的. 如果 $e>1$，由伽罗瓦理论易知 E 包含 $\Phi(\sqrt{-1})$ 上的子域 Γ 使得 $[\Gamma: \Phi(\sqrt{-1})]=2$. 但这与前面已证明的结果相矛盾. 故 $e=1$，那么 $[E:\Phi]=2, E=\Phi(\sqrt{-1})$. 这就证明了 $\Phi(\sqrt{-1})$ 是 $(x^2+1)f(x)$ 的一个分裂域，而且 $f(x)$ 在 $\Phi(\sqrt{-1})$ 中有根. 因此，$\Phi(\sqrt{-1})$ 是代数闭的.

如果 Φ 是一个实闭域，则我们已证过 Φ 只能用一种方法使之序化，定理 2 的证明指出这个序应这样规定：如果 $\alpha=\beta^2, \beta\neq 0$，则 $\alpha>0$. 因此，每个实闭域都是可以序化的，而且满足定理 5 的条件(1). 定理 4 表明每个实闭域满足定理 5 的条件(2). 故有下述的

推论. 如果 Φ 是实闭域，则 $\sqrt{-1}\notin\Phi$，而且 $\Phi(\sqrt{-1})$ 是代数闭的.

下面我们证明此推论的逆命题，即

定理 6. 如果 Φ 是一个域，$\sqrt{-1}\notin\Phi$ 而 $\Phi(\sqrt{-1})$ 是代数闭的，则 Φ 是实闭的.

证 设 Φ 满足条件. 首先，我们要注意 $\Phi[x]$ 中正次数不可约多项式的次数是 1 或 2. 设 $f(x)$ 是这样的多项式，θ 是 $f(x)$ 含于 $\Omega=\Phi(\sqrt{-1})$ 中的一个根，则 $[\Phi(\theta):\Phi]=\deg f(x)$，$[\Phi(\theta):\Phi]\leqslant[\Omega:\Phi]=2$. 因此，如所断言的 $\deg f(x)=1$ 或 2. 今设 $\alpha, \beta\neq 0\in\Phi$，并考虑多项式

$$
\begin{aligned}
(2)\qquad g(x)&=(x^2-\alpha)^2+\beta^2=(x^2-\alpha-\beta i)(x^2-\alpha+\beta i)\\
&=(x-(\alpha+\beta i)^{1/2})(x+(\alpha+\beta i)^{1/2})\cdot\\
&\quad(x-(\alpha-\beta i)^{1/2})(x+(\alpha-\beta i)^{1/2}),
\end{aligned}
$$

其中 $i=\sqrt{-1}$. 此多项式属于 $\Phi[x]$，但由于 $\pm\alpha\pm\beta i\notin\Phi$，此多项式在 $\Phi[x]$ 中没有一次因式. 于是 $g(x)$ 是两个不可约二次多项式之积. 因为 $\alpha+\beta i\notin\Phi$，故被 $x-(\alpha+\beta i)^{1/2}$ 整除的那个不可约的二次多项式不能是

$$(x-(\alpha+\beta i)^{1/2})(x+(\alpha+\beta i)^{1/2})=x^2-(\alpha+\beta i);$$

因此，问题中的多项式或者是

$$(x-(\alpha+\beta i)^{1/2})(x-(\alpha-\beta i)^{1/2}),$$

或者是

$$(x-(\alpha+\beta i)^{1/2})(x+(\alpha-\beta i)^{1/2}).$$

这两种可能都说明 $(\alpha^2+\beta^2)^{1/2}\in\Phi$. 由于 α 和 β 是 Φ 的任意非零元，我们证明了 Φ 中两个元的平方和是一个元的平方. 由归纳法可证 Φ 中每个平方和仍是一个平方. 由于 -1 不是 Φ 的一个元的平方，故 -1 不是 Φ 中元的平方和，故 Φ 是形式实域. 如果 P 是 Φ 的一个真代数扩张域，则 P 同构于 $\Omega=\Phi(\sqrt{-1})$. 故 P 不是形式实域，因此 Φ 是实闭的. 定理 6 证毕.

定理 5 的推论和定理 6 给出了实闭域内下列性质刻划：$\sqrt{-1}\notin\Phi$ 和 $\Phi(\sqrt{-1})$ 是代数闭的. 我们也注意到在我们的论证中还给出了另一个刻划，即一个有序域是实闭的当且仅当它满足定理 5 的条件(1)和(2)，就是说，Φ 的正元在 Φ 中有平方根而且 Φ 上的奇次多项式在 Φ 中有根. 这容易从我们的结果中导出. 下面，我们给出如下由实闭域刻划得出的有用的结果.

推论. 如果 P 是域 Φ 的一个实闭扩张域，则 P 中在 Φ 上的代数元所成的子域 A 是实闭域.

证. 设 $\Omega=\mathrm{P}(\sqrt{-1})$，则 Ω 是代数闭的. 因此 Ω 中在 Φ 上是代数的元所成的子域 Γ 是代数闭的. 如果 $\alpha+\beta\sqrt{-1}(\alpha,\ \beta\in\mathrm{P})$ 属于 Γ，则 $\alpha-\beta\sqrt{-1}$ 也属于 Γ. 因此 $\alpha=\frac{1}{2}(\alpha+\beta\sqrt{-1}+\alpha-\beta\sqrt{-1})\in\Gamma$. 所以 $\beta\in\Gamma$. 由于 $\alpha,\beta\in\mathrm{P}$，则 $\alpha,\beta\in A$. 由此得 $\Gamma=A(\sqrt{-1})$. 因为 $\sqrt{-1}\notin A$，我们知道 A 满足定理 6 的条件；故 A 是一个实闭域.

习 题 47

1. 设 Ω/Φ 是代数闭的，Φ 为形式实域. 证明 Ω/Φ 含有一个实闭子域 P/Φ 使得 $\Omega=P(\sqrt{-1})$. 特别地，证明每个特征为 0 的代数闭域含有实闭子域 P 使得 $\Omega=P(\sqrt{-1})$.

3. 斯图姆 (Sturm) 定理 这一节我们将得到一个古典的结

果即斯图姆定理，它使我们能决定多项式方程 $f(x)=0$ 在一个实闭域中根的精确个数．此结果是后续内容的基础．在推导中我们将主要采用韦伯在他的著作《代数学教程》(Lehrbuch der Algebra) (1898)卷 I，pp. 301—313 的论述方法． 首先需要下列基本结果．

引理． 设 Φ 是一个实闭域，$f(x)$ 是系数在 Φ 中的多项式．假设 α, β 是 Φ 的元使得 $f(\alpha)<0$ 而 $f(\beta)>0$，则在 α 和 β 间存在一个 γ 使得 $f(\gamma)=0$．

证 我们知道，在 $\Phi[x]$ 中仅有的不可约多项式是一次和二次的多项式．设 $g(x)=x^2+\mu x+\nu\in\Phi[x]$ 是不可约的．则必须有 $\mu^2-4\nu<0$．由二次方程的求根公式这是明显的．现可设 $4\nu-\mu^2=4\delta^2$，而 δ 是 Φ 的一个非零元，且有

$$(3)\qquad g(x)=x^2+\mu x+\nu=\left(x+\frac{\mu}{2}\right)^2+\delta^2.$$

显然，此公式表明对 Φ 的每个 η 有 $g(\eta)>0$．现设 $f(x), \alpha, \beta$ 如定理所述．在 $\Phi[x]$ 中，我们有因式分解

$$(4)\qquad (x)=\rho(x-\rho_1)(x-\rho_2)\cdots(x-\rho_k)g_1(x)\cdots g_l(x)$$

而 $g_i(x)$ 为首项系数为 1 的不可约二次多项式． 设没有一个 ρ_i 在 α 和 β 之间．则对每个 i，$\alpha-\rho_i$ 和 $\beta-\rho_i$ 的符号相同(两者为正或两者为负)． 因为 $g_j(\alpha)>0$ 和 $g_j(\beta)>0(1\leqslant j\leqslant l)$，由此得 $f(\alpha)$ 和 $f(\beta)$ 有相同的符号，这与题设矛盾，故有一个 ρ_i 在 α 和 β 之间．证毕．

设 Φ 是一个实闭域，$f(x)$ 是一个系数在 Φ 中的正次数的多项式，按韦伯的说法，称多项式序列

$$(5)\qquad f_0(x)=f(x), f_1(x), \cdots, f_s(x)$$

为多项式 $f(x)$ 关于区间 $[\alpha,\beta]$ (即 $\alpha\leqslant x\leqslant\beta$)的**斯图姆序列**，如果 $f_i(x)\in\Phi[x]$ 且满足下述条件：

(i) $f_s(x)$ 在$[\alpha,\beta]$中没有根．

(ii) $f_0(\alpha)\neq 0, f_0(\beta)\neq 0$．

(iii) 如果 $\gamma\in[\alpha,\beta]$ 是 $f_j(x)$ 的一个根，$0<j<s$，则

$$f_{i-1}(\gamma)f_{i+1}(\gamma) < 0.$$

(iv) 如果 $f(\gamma) = 0, \gamma \in [\alpha, \beta]$，则存在区间 $\gamma_1 \leqslant x < \gamma$ 和 $\gamma < x \leqslant \gamma_2$ 使得对第一个区间的 x 有 $f_0(x)f_1(x) < 0$，对第二个区间的 x 有 $f_0(x)f_1(x) > 0$.（总之，$f_0(x)f_1(x)$ 在 $x = \gamma$ 处是 x 的增函数.）

我们要对有不同根的任意多项式证明这种序列的存在性．但首先我们要看一看如何利用这种序列来决定 $f(x)$ 在开区间(α,β)（即 $\alpha < x < \beta$）内根的个数．考虑Φ中元的序列

(6) $$f_0(\alpha),f_1(\alpha),\cdots,f_s(\alpha), \qquad f_0(\beta),f_1(\beta),\cdots,f_s(\beta)$$

的变号数，如果 $\gamma = \{\gamma_1,\gamma_2,\cdots,\gamma_m\}$是$\Phi$中非零元的有限序列，则定义$\gamma$的**变号数**为使得 $\gamma_i\gamma_{i+1} < 0$ 的 i 之个数 $(1 \leqslant i \leqslant m-1)$．若 $\gamma = \{\gamma_1,\gamma_2,\cdots,\gamma_m\}$ 是Φ中元的任一序列，定义γ的变号数为去掉γ中的 0 后得到的简缩序列的变号数．例如

$$\{1,0,0,2,-1,0,3,4,-2\}$$

有三个变号数．

于是我们可以叙述

定理 7. 设 $f(x)$ 是一个系数在实闭域Φ内的正次数多项式，$f_0(x) = f(x),f_1(x),\cdots,f_s(x)$ 是 $f(x)$ 关于区间 $[\alpha, \beta]$ 的斯图姆序列，则 $f(x)$ 在 (α,β) 中不同根的个数为 $V_\alpha - V_\beta$，而 V_γ一般表示序列 $\{f_0(\gamma),f_1(\gamma),\cdots,f_s(\gamma)\}$ 的变号数．

证 把区间$[\alpha,\beta]$用给定的斯图姆序列的多项式 $f_i(x)$ 的根分成子区间．于是有序列 $\alpha = \alpha_0 < \alpha_1 < \cdots < \alpha_m = \beta$，使得没有一个 $f_j(x)$ 在 (α_i,α_{i+1}) 中有根．选择 $\alpha_i' \in (\alpha_{i-1}, \alpha_i)$，$1 \leqslant i \leqslant m$（例如，$\alpha_i' = \frac{1}{2}(\alpha_{i-1}+\alpha_i)$），并设 $V_{\alpha_i'}$ 是序列 $\{f_j(\alpha_i'), j = 0,1,\cdots,s\}$ 的变号数．显然

$$V_\alpha - V_\beta = V_\alpha - V_{\alpha_1'} + \sum_1^{m-1}(V_{\alpha_i'} - V_{\alpha_{i+1}'}) + V_{\alpha_m'} - V_\beta,$$

故我们尝试计算 $V_\alpha - V_{\alpha_1'}, V_{\alpha_i'} - V_{\alpha_{i+1}'}, V_{\alpha_m'} - V_\beta$ 的值．我们知道 $f_0(\alpha) \neq 0$，$f_0(\beta) \neq 0, f_s(\alpha_i) \neq 0$，$f_s(\alpha_i') \neq 0$．首先假设没有

$f_j(\alpha)=0, 0<j<s$，则 $f_k(\alpha)f_k(\alpha_1')>0$，对 $k=0,\cdots,s$。因为否则由引理知 $f_k(x)$ 之一在 (α,α_1') 中有根，但这与区间(α_i,α_{i+1})的性质矛盾。故对所考虑的情形有 $V_\alpha=V_{\alpha_1'}$。其次，对某个 j，$0<j<s$，设 $f_j(\alpha)=0$，则由 (iii) 知 $f_{j-1}(\alpha)\cdot f_{j+1}(\alpha)<0$。由于 $f_{j-1}(x)$ 和 $f_j(x)$ 在 (α,α_1) 中没有根，得到 $f_{j-1}(\alpha)f_{j-1}(\alpha_1')>0$ 和$f_{j+1}(\alpha)\ f_{j+1}(\alpha_1')>0$。因此 $f_{j-1}(\alpha_1')\ f_{j+1}(\alpha_1')<0$。由此得知 $f_{j-1}(\alpha),0,f_{j+1}(\alpha)$ 和 $f_{j-1}(\alpha_1'),f_j(\alpha_1'),f_{j+1}(\alpha_1')$ 分别对 V_α 和 $V_{\alpha_1'}$ 产生相同的变号数，考虑一切 j 后可见 $V_\alpha-V_{\alpha_1'}=0$。类似的讨论表示 $V_{\alpha_m'}-V_\beta=0$。同样的讨论还可证明，如果 $\alpha_i(1\leqslant i\leqslant m-1)$ 不是 $f(x)=f_0(x)$ 的根，则又有 $V_{\alpha_i'}-V_{\alpha_{i+1}'}=0$。剩下的是考虑当 $f(\alpha_i)=0(1\leqslant i\leqslant m-1)$ 时的情况。由 (iv) 和 α_i' 的选择有 $f_0(\alpha_i')f_1(\alpha_i')<0$ 和 $f_0(\alpha_{i+1}')f_1(\alpha_{i+1}')>0$。则当序列 $f_0(\alpha_{i+1}),f_1(\alpha_{i+1}')$ 没有变号时序列 $f_0(\alpha_i')$，$f_1(\alpha_i')$ 有一个变号。上述论证表明：如果 $j>1,f_{j-1}(\alpha_i'),f_j(\alpha_i')$，$f_{j+1}(\alpha_i')$ 和 $f_{j-1}(\alpha_{i+1}')$，$f_j(\alpha_{i+1}')$，$f_{j+1}(\alpha_{i+1}')$ 有相同的变号数，故若 $f(\alpha_i)=0$ 则 $V_{\alpha_i'}-V_{\alpha_{i+1}'}=1$。因此，我们证明了根据 $f(\alpha_i)\neq 0$ 或 $f(\alpha_i)=0$ 有 $V_{\alpha_i'}-V_{\alpha_{i+1}'}=0$ 或 1。故

$$V_\alpha-V_\beta=V_\alpha-V_{\alpha_1'}+\sum_1^{m-1}(V_{\alpha_i'}-V_{\alpha_{i+1}'})+V_{\alpha_m'}-V_\beta$$

是使得 $f(\alpha_i)=0$ 的 α_i 的个数。

现设 $f(x)$ 是一个任意多项式。定义 $f(x)$ 的**标准序列**为

$$\begin{aligned}
&f_0(x)=f(x),\quad f_1(x)=f'(x)\quad (f(x)\text{ 的形式导数}),\\
&f_0(x)=q_1(x)f_1(x)-f_2(x),\qquad \deg f_2<\deg f_1\\
(7)\qquad &\vdots\\
&f_{i-1}(x)=q_i(x)f_i(x)-f_{i+1}(x),\quad \deg f_{i+1}<\deg f_i\\
&\vdots\\
&f_{s-1}(x)=q_s(x)f_s(x).
\end{aligned}$$

因此 $f_i(x)$ 是通过将求 $f(x)$ 与 $f'(x)$ 的最高公因式的辗转相除法加以修改而得到的。此法每步末尾的多项式是将除法过程中所得的余式取负号的结果。显然 $f_s(x)$ 是 $f(x)$ 和 $f'(x)$ 的最高公

因式，而且还是一切 $f_i(x)$ 的因式。于是设 $g_i(x)=f_i(x)f_s(x)^{-1}$ 并考察序列

(8) $$g_0(x),g_1(x),\cdots,g_s(x).$$

我们着手证明此序列是 $g_0(x)$ 关于任一个使 $g_0(\alpha)\neq 0$，$g_0(\beta)\neq 0$ 的区间 $[\alpha,\beta]$ 的斯图姆序列。显然斯图姆序列定义中的 (ii) 是满足的。由于 $g_s(x)=1$，(i) 也是满足的。用 $f_s(x)$ 除 (7) 中的多项式得关系式 $g_{j-1}(x)=q_j(x)g_j(x)-g_{j+1}(x)$，$0<j<s$。假设 $g_j(\gamma)=0$，则 $g_{j-1}(\gamma)\neq 0$ 和 $g_{j+1}(\gamma)\neq 0$，因为否则此关系式表明将从某一个起所有的 $g_k(\gamma)=0$，此与 $g_s(x)=1$ 矛盾。因此 $g_{j-1}(\gamma)g_{j+1}(\gamma)\neq 0$，而且由于 $g_{j-1}(\gamma)=g_j(\gamma)\cdot q_j(\gamma)-g_{j+1}(\gamma)=-g_{j+1}(\gamma)$ 得 $g_{j+1}(\gamma)g_{j-1}(\gamma)<0$，故 (iii) 成立。现设 γ 在$[\alpha,\beta]$中有 $g_0(\gamma)=0$。则 $f(x)=(x-\gamma)^e h(x)$，$e>0$，$h(\gamma)\neq 0$ 和 $f'(x)=(x-\gamma)^e h'(x)+e(x-\gamma)^{e-1}h(x)$。而且 $f_s(x)=(x-\gamma)^{e-1}k(x)$，其中 $k(\gamma)\neq 0$。因此 $h(x)=k(x)l(x)$，其中 $l(x)\neq 0$，$h'(x)=k(x)m(x)$。由这些关系式得

(9) $$g_0(x)=(x-\gamma)l(x),\qquad l(\gamma)\neq 0,$$
$$g_1(x)=(x-\gamma)m(x)+el(x),$$

那么 $g_1(\gamma)=el(\gamma)\neq 0$。现选择一个区间 $[\gamma_1,\gamma_2]$，使 γ 含于其内部，而且在 $[\gamma_1,\gamma_2]$ 中有 $l(x)\neq 0$，与 $g_1(x)\neq 0$。则由引理得 $g_1(x)$ 和 $l(x)$ 在 $[\gamma_1,\gamma_2]$ 中或者均为正或者均为负，因而在 $[\gamma_1,\gamma_2]$ 中有 $g_1(x)l(x)>0$。故 $g_0(x)\,g_1(x)=(x-\gamma)g_1(x)l(x)$ 与 $x-\gamma$ 在 $[\gamma_1,\gamma_2]$ 中有相同的符号，即在 $\gamma_1\leqslant x<\gamma$ 时，$g_0(x)g_1(x)<0$，而在 $\gamma<x\leqslant\gamma_2$ 时，$g_0(x)g_1(x)>0$。这表明 (iv) 成立，因此(8)是 $g_0(x)$ 的斯图姆序列。

如果 $f(x)$ 没有重根，则1可作为 $f(x)$ 和 $f'(x)$ 的最高公因式。因而序列 $\{f_0(x),f_1(x),\cdots,f_s(x)\}$ 与 $\{g_0(x),g_1(x),\cdots,g_s(x)\}$ 相差一个 Φ 中的非零因子，所以序列 $f_i(x)$ 是 $f(x)=f_0(x)$ 的斯图姆序列。如果 $f(x)$ 有重根，则标准序列(7)对于包含一个重根的区间不会是斯图姆序列，尽管如此，我们仍然可以用标准序

列去决定 $f(x)$ 在 (α,β) 中的不同根的个数. 这就是斯图姆定理的内容

斯图姆定理. 设 $f(x)$ 是任一系数在实闭域 Φ 内的正次数多项式,$\{f_0(x)=f(x),f_1(x)=f'(x),\cdots,f_s(x)\}$ 是 $f(x)$ 的标准序列(7). 假设 $[\alpha,\beta]$ 是使 $f(\alpha)\neq 0,f(\beta)\neq 0$ 的一个区间. 则 $f(x)$ 在 $[\alpha,\beta]$ 内不同根的个数为 $V_\alpha-V_\beta$,这里 V_γ 表示 $\{f_0(\gamma),f_1(\gamma),\cdots,f_s(\gamma)\}$ 的变号数.

证 设 $g_i(x)=f_i(x)f_s(x)^{-1}$ 如上规定,如果不计重数,多项式 $f(x)$ 和 $g_0(x)$ 在 (α,β) 中有相同的根(§1.6,习题的第 7 题). 由于序列 $\{g_i(x)\}$ 是 $g_0(x)$ 的斯图姆序列, 则这些根的个数为 $V_\alpha(g)-V_\beta(g)$,这里 $V_\gamma(g)$ 是 $\{g_i(x)\}$ 的变号数. 因为

$$f_i(\gamma)=g_i(\gamma)f_s(\gamma) \text{ 和 } f_s(\alpha)\neq 0,f_s(\beta)\neq 0,$$

显然有 $V_\alpha(g)=V_\alpha$, $V_\beta(g)=V_\beta$. 因此 $V_\alpha-V_\beta$ 是 $f(x)$ 在 (α,β) 内不同根的个数.

我们知道 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ 在 Φ 内的根是在区间$[-M,M]$内的,而 $M=\max(1,|a_1|+|a_2|+\cdots+|a_n|)$(§1,习题的第 3 题). 若我们设 $\mu=1+|a_1|+\cdots+|a_n|$, 则 $f(x)$ 在 Φ 内的根在 $(-\mu,\mu)$ 内. 如果 $f_0(x)=f(x),f_1(x),\cdots,f_s(x)$ 是 $f(x)$ 的标准序列(7),则 $f(x)$ 在 Φ 内根的个数为 $V_{-\mu}-V_\mu$,这里 V_γ 是 $\{f_0(\gamma),f_1(\gamma),\cdots,f_s(\gamma)\}$ 的变号数. 这就得到了决定 $f(x)$ 在 Φ 中根的个数的一种构造方法. 有时使用界 η 代替 μ 更好一些,这里 η 是 a_i 的一个多项式. 为此目的,我们注意到 $1+a_i^2>|a_i|$, 所以可以取 $\eta=1+\sum(1+a_i^2)=(n+1)+\sum a_i^2$. 则在 Φ 内的根均落在 $(-\eta,\eta)$ 中.

习 题 48

在下面各题中 Φ 均为实闭域.

1. 证明罗尔 (Rolle) 定理: 如果 $f(x)\in\Phi[x]$ 在 Φ 内有根 α, β, 则存在 $\gamma\in\Phi$, $\alpha<\gamma<\beta$ 使得 $f'(\gamma)=0$.

2. 证明多项式的中值定理: 如果 $\alpha<\beta$, 则存在一个 γ, $\alpha<\gamma<\beta$, 使得 $f(\beta)-f(\alpha)=(\beta-\alpha)f'(\gamma)$.

3. 证明 $f(x)$ 在任一闭的有限区间 $[\alpha,\beta]$ 上有极大值.

4. (布丹 (Budan) 定理). 设 $f(x)$ 有次数 n, $\alpha<\beta$ 在 Φ 内但均不是 $f(x)$ 的根, W_γ 表示序列 $f(\gamma), f'(\gamma), \cdots, f^{(n)}(\gamma)$ 的变化数. 证明 $W_\alpha - W_\beta$ 比 $f(x)$ 在 Φ 内属于 (α,β) 的根的个数(计及根的重数)多一个非负偶数.

5. 由第 4 题得笛卡尔 (Descartes') 规则: 设 $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \cdots + \alpha_l x^{n-l}$, $\alpha_0 \neq 0$, $\alpha_l \neq 0$, $\alpha_i \in \Phi$. 设 P 表示序列 $(\alpha_0, \alpha_1, \cdots, \alpha_l)$ 的变号数. 证明 P 比 $f(x)$ 的正根个数(计及根的重数)多一个非负偶数.

4. 有序域的实闭包 我们知道每个形式实域均能嵌入一个实闭域中. 特别,这可用于有序域. 现在我们将证明,如果 Φ 是一个有序域,则存在 Φ 的一个实闭代数扩张域 Δ,使 Δ 的(唯一)的序是 Φ 的序的扩张. 此外,我们将知道 Δ 在本质上是唯一的. 为了证明 Δ 的存在性,我们需要下述的

引理. 设 Φ 是一个有序域, Ω 是 Φ 的代数闭包, E 是 Ω/Φ 的子域,它是添加 Φ 的正元的平方根到 Φ 而得到的,则 E 是形式实域.

证. 假设在 E 中有关系式 $\Sigma\xi_i^2 = 0$, 则 ξ_i 包含在形如 $\Phi(\sqrt{\beta_1}, \sqrt{\beta_2}, \cdots, \sqrt{\beta_r})$ 的有限维扩张域内, 其中 β_i 为 Φ 的正元. 因此,只要证明 E 的每个子域 $\Phi(\sqrt{\beta_1}, \sqrt{\beta_2}, \cdots, \sqrt{\beta_r})$, $\beta_i > 0$ 是形式实域就够了. 我们对子域的维数用归纳法来证明: 对此, 证明表面上更强的命题是方便的: 对 Φ 中的 $\gamma_i > 0$ 和 $\Phi(\sqrt{\beta_1}, \sqrt{\beta_2}, \cdots, \sqrt{\beta_r})$ 中的 ξ_i,如果 $\Sigma\gamma_i\xi_i^2 = 0$,则每个 $\xi_i = 0$. 因为 Φ 是一个有序域,对于 Φ 来说, 这点是显然的. 假设对于维数比 $\Gamma = \Phi(\sqrt{\beta_1}, \cdots, \sqrt{\beta_r})$ 低的给定形式的子域命题成立. 可设 $\Gamma \supset H = \Phi(\sqrt{\beta_1}, \cdots, \sqrt{\beta_{r-1}})$, 而对 H 结论成立. 于是设 $\Sigma\gamma_i\xi_i^2 = 0$, $\xi_i \in \Gamma$, $\gamma_i > 0$, $\gamma_i \in \Phi$. 记 $\xi_i = \eta_i + \zeta_i\sqrt{\beta_r}$, η_i, $\zeta_i \in H$,则 $\Sigma\gamma_i\eta_i^2 + \Sigma\beta_r\gamma_i\zeta_i^2 + 2(\Sigma\gamma_i\eta_i\zeta_i)\sqrt{\beta_r} = 0$. 由于 $\sqrt{\beta_r} \notin H$, $\Sigma\gamma_i\eta_i\zeta_i = 0$ 故 $\Sigma\gamma_i\eta_i^2 + \Sigma\beta_r\gamma_i\zeta_i^2 = 0$. 由于 γ_i, $\beta_r\gamma_i \in \Phi$, $\gamma_i > 0$, $\beta_r\gamma_i > 0$ 和 $\eta_i, \zeta_i \in H$, 则每个 η_i 和 $\zeta_i = 0$. 从而每个 $\xi_i = 0$,故结论对 Γ 也成立.

定义 4. 设 Φ 是一个有序域, 则 Φ 的一个扩张域 Δ 称为 Φ 的一个实闭包,如果(1) Δ 是实闭域,(2) Δ 在 Φ 上是代数的,(3) Δ 的

序是Φ的序的一个扩张.

现在我们可证明下述的基本结果.

定理 8. 每个有序域Φ都有一个实闭包. 如果 Φ_1 和 Φ_2 是有序域,Δ_1,Δ_2 分别是它们的实闭包,则 Φ_1 到 Φ_2 上的任一序同构均能唯一地扩张成 Δ_1 到 Δ_2 上的同构. 且此扩张是一个序同构.

证 设Φ是一个有序域, Ω是Φ的一个代数闭包. 设E是Ω的子域, 它是添加Φ的一切正元的平方根到Φ上得到的. 则E是形式实域, Ω是E的一个代数闭包. 我们已经知道存在 Ω/E 的一个实闭子域Δ(定理3). 设 $\beta\in\Phi,\beta>0$. 则 $\beta=\rho^2,\rho\in\Delta$. 故在$\Delta$中 $\beta>0$, 那么Δ中的序是Φ的序的一个扩张. 因此Δ是Φ的一个实闭包.

其次设 $\Phi_i(i=1,2)$ 是有序域, Δ_i 是 Φ_i 的一个实闭包, $\alpha\to\bar{\alpha}$ 是 Φ_1 到 Φ_2 上的一个序同构. 我们希望把给定的同构扩张成 Δ_1 到 Δ_2 上的同构. 首先注意,如果 $f(x)\in\Phi_1[x]$,则 $f(x)$ 和它在 $\alpha\to\bar{\alpha}$ 之下的象 $\bar{f}(x)$ 分别在 Δ_1 和 Δ_2 中根的个数相同. 我们知道在 Φ_1 中存在$\mu>0$使得$f(x)$在Δ_1 中每个根含于$(-\mu,\mu)$ 中, 而且由斯图姆定理知, $f(x)$ 在 Δ_1 中并落在区间$(-\mu,\mu)$中的根的个数,也就是$f(x)$在Δ_1 中根的总数等于 $V_{-\mu}-V_{\mu}$, 这里 V_γ 是 f 的标准序列(7)在γ处的变号数. 由于f的标准序列含于 $\Phi_1[x]$ 中, 所有这一切对 $\bar{f}(x)$ 和 Δ_2 亦成立. 故 $\bar{f}(x)$ 在 Δ_2 中根的个数与 $f(x)$ 在 Δ_1 中根的个数相同. 其次注意,如果 $F=\{\rho_1,\rho_2,\cdots,\rho_n\}$ 是 Δ_1 的一个有限子集, 则存在 Δ_1/Φ 中包含F的子域 Γ_1 和 Γ_1 到 Δ_2 内的一个同构 τ, 它是 $\alpha\to\bar{\alpha}$ 的扩张并使得: 若 $\rho_1<\rho_2<\cdots<\rho_n$,则 $\rho_1^\tau<\rho_2^\tau<\cdots<\rho_n^\tau$. 为此,令 $f(x)$ 是 $\Phi_1[x]$ 中的一个多项式, 使元 $\rho_i(1\leqslant i\leqslant n)$, $\sigma_j=\sqrt{\rho_{j+1}-\rho_j}\,(1\leqslant j\leqslant n-1)$,为 $f(x)$ 的部分根.我们注意到由于 Δ_1 是实闭域和 $\rho_{j+1}-\rho_j>0$,因此有 $\sigma_j\in\Delta_1$ (定理 2 的证明). 设 Γ_1 是 Φ_1 的由 $f(x)$ 在 Δ_1 中的根生成的有限维扩张,则 $\Gamma_1=\Phi_1(\theta_1)$, 而且若 $g(x)$ 是 θ_1 在 Φ_1 上的最小多

项式，那么 $\bar{g}(x)$ 在 Δ_2 中有一个根 θ_2. 我们有一个 Γ_1 到 $\Phi_2(\theta_2)$ 上的同构使得 $\alpha^{\tau}=\bar{\alpha},\alpha\in\Phi_1$，而且 $\theta_1^{\tau}=\theta_2$. 则 $\rho_{i+1}^{\tau}-\rho_i^{\tau}=(\rho_{i+1}-\rho_i)^{\tau}=(\sigma_i\tau)^2>0$，故在 Δ_2 中如所要求的那样有 $\rho_1^{\tau}<\rho_2^{\tau}<\cdots<\rho_m^{\tau}$. 现在如下定义 Δ_1 到 Δ_2 内的一个映射 η：设 ρ 是 Δ_1 的一个元，$h(x)$ 是 ρ 在 Φ_1 上的最小多项式. 设 $h(x)$ 在 Δ_1 中的根为 $\rho_1<\rho_2<\cdots<\rho_m$，并设 $\rho_k=\rho$. 则 $\bar{h}(x)$ 在 Δ_2 中恰有 m 个根 $\rho_1'<\rho_2'<\cdots<\rho_m'$，并令 $\rho^{\eta}=\rho_k'$. 显然 $\alpha^{\eta}=\bar{\alpha},\alpha\in\Phi_1$，并易知 η 是 1—1 的和满射的. 我们断言，若 $\rho,\sigma\in\Delta_1$，则 $(\rho+\sigma)^{\eta}=\rho^{\eta}+\sigma^{\eta},(\rho\sigma)^{\eta}=\rho^{\eta}\sigma^{\eta}$，因而 η 是 Δ_1 到 Δ_2 内的同构，是 $\alpha\to\bar{\alpha}$ 的扩张. 设 F 是 Δ_1 的一个有限子集，它包含 $\rho,\sigma,\rho+\sigma$ 和 $\rho\sigma$ 在 Φ_1 上最小多项式在 Δ_1 中的根. 我们已知存在一个 Φ_1 上包含 F 的 Δ_1 的子域 Γ_1 和存在一个 Γ_1 到 Δ_2 内且为 $\alpha\to\bar{\alpha}$ 的扩张的能保持 F 中元的序的同构 τ，与前面一样，设 $h(x)$ 是 ρ 在 Φ_1 上的最小多项式，并设 $\rho_1<\rho_2<\cdots<\rho_m$ 是 $h(x)$ 含于 Δ_1 中的根，则 $\rho_i\in F$，而且 $\rho_1^{\tau}<\rho_2^{\tau}<\cdots<\rho_m^{\tau}$，故 $\bar{h}(\rho_i^{\tau})=0$，并由 η 的定义得 $\rho^{\eta}=\rho^{\tau}$. 类似地有 $\sigma^{\eta}=\sigma^{\tau},(\rho+\sigma)^{\eta}=(\rho+\sigma)^{\tau}$，$(\rho\sigma)^{\eta}=(\rho\sigma)^{\tau}$. 因为 τ 是一个同构，由此得 $(\rho+\sigma)^{\eta}=\rho^{\eta}+\sigma^{\eta},(\rho\sigma)^{\eta}=\rho^{\eta}\sigma^{\eta}$. 所以 η 是 Δ_1 到 Δ_2 上的一个同构，并且还是给定的 Φ_1 到 Φ_2 上的同构的扩张. 现设 η' 是 Δ_1 到 Δ_2 上的任意同构，因为 η' 把平方映成平方，显然 η' 是个序同构，再设 η' 是映射 $\alpha\to\bar{\alpha}$ 的扩张. 设 $\rho\in\Delta_1,\rho_1<\rho_2<\cdots<\rho_m$ 是 ρ 在 Φ_1 上的最小多项式 $h(x)$ 在 Δ_1 内的根，则 $\rho_1^{\eta'}<\rho_2^{\eta'}<\cdots<\rho_m^{\eta'}$ 是 $\bar{h}(x)$ 在 Δ_2 内的根，由此得 $\rho^{\eta'}=\rho^{\eta}$. 故扩张 η 是唯一的. 证毕.

如果 Δ_1 和 Δ_2 是给定有序域 Φ 的两个实闭包，则 Φ 上的恒等映射可以扩张成 Δ_1 到 Δ_2 上的一个序同构. 在此意义下，实闭包是等价的，因此我们可以说"Φ 的实闭包".

习　题　49

1. 设 Φ 是一个有序域，Λ 是一个扩张域，使得关系式 $\Sigma\gamma_i\xi_i^2=0$ 仅当每个 $\xi_i=0$ 时才成立，这里 γ_i 是 Φ 的正元，$\xi_i\in\Lambda$. 证明可以把 Λ 有序化，并使它的序是 Φ 的序的一个扩张.

2. 设Φ是个有序域，A是一个实闭扩张域，其序是Φ的序的一个扩张. 证明A包含Φ的一个实闭包.

5. 实代数数 我们知道有理数域 R_0 有一个唯一的序(§1, 习题的第 1 题)，此有序域有一个在同构意义下唯一确定的实闭包 Δ_0，我们将称 R_0 的任一实闭包 Δ_0 为实代数数域. 显然 $\Omega_0=\Delta_0(\sqrt{-1})$是 R_0 的一个代数闭包，我们将称此域为代数数域

现设 $\Gamma=R_0(\theta)$ 是有理数域的一个有限维扩张域，则若 $n=[\Gamma:R_0]$，我们有 n 个不同的 Γ/R_0 到 Ω_0/R_0 内的同构映射. 这些同构由映射 $\theta\to\theta_i(1\leqslant i\leqslant n)$ 所决定，其中 $\{\theta_1,\theta_2,\cdots,\theta_n\}$ 是θ的最小多项式 $g(x)$在 Ω_0 内根的集. 设 $\theta_1,\theta_2,\cdots,\theta_r$ 是属于 Δ_0 的那些 θ_i. 我们将称这些 θ_i 为 θ 的实共轭. 如果 θ 没有实共轭，我们约定 $r=0$. 设 $\tau_i(1\leqslant i\leqslant r)$ 是 Γ/R_0 到 Δ_0/R_0 内的同构使 $\theta^{\tau_i}=\theta_i$，则 $R_0(\theta_i)\subseteq\Delta_0$ 的序由 Δ_0 中唯一的序所决定，并给出 Γ 的一个序：对 $\rho\in\Gamma$，规定 $\rho>0$ 当且仅当 $\rho^{\tau_i}>0$. 我们将把 Γ 的这个序看作是由 τ_i 所决定的序. 现设 Γ 有任意序，Δ 为 Γ 关于这个序的一个实闭包. 因为 Γ 在 R_0 上是代数的，显然 Δ 是 R_0 的一个实闭包. 所以，我们有 Δ/R_0 到 Δ_0/R_0 上的一个序同构 τ. τ 在 Γ 上的限制与 τ_i 中的某一个重合，显然，给定的 Γ 的序由 τ_i 决定的序相同. 最后，设 τ_i 和 τ_j 决定 Γ 的相同的序，则有一个 $R_0(\theta_i)$ 到 $R_0(\theta_j)$ 上的保序同构使得 $\theta_i\to\theta_j$. 因为 Δ_0 是 $R_0(\theta_i)$和 $R_0(\theta_j)$ 的实闭包，由定理 8，存在 Δ_0 在 R_0 上的一个自同构使 θ_i 对应 θ_j. 另一方面，因为 Δ_0 是 R_0 的一个实闭包. 定理 8 还表明恒等映射是 Δ_0 在 R_0 上仅有的自同构. 故必定有 $\theta_j=\theta_i$. 这些结果建立下述的

定理 9. 设 Γ 是有理数域的一个有限维扩张，则 Γ 的不同序的个数与 Γ/R_0 到实代数数域 Δ_0/R_0 内的同构的个数相等.

特别，Γ 的不同序的个数不能超过$[\Gamma:R_0]$，而且 $\Gamma=R_0(\theta)$没有序当且仅当 θ 关于 R_0 的最小多项式没有实根，即在 Δ_0 中没有根.

现在我们应用此结果去得到希尔伯特和兰道定理，该定理给

出了 $\Gamma = R_0(\theta)$(θ 为代数元)的元为此域中元的平方和的充分必要条件. 首先,设Φ为任一个特征$\neq 2$的域,而且如在§1中一样,令$\Sigma(\Phi)$ 是Φ的形如 $\Sigma\alpha_i^2$ 的元之子集,$\alpha_i \in \Phi$. 其次,我们引进下述定义.

定义 5. 称域的一个元 ρ 为全正的,如果在这个域的每种序中 $\rho > 0$.

特别,对没有序的域应理解为其每个元都是全正的.因此,非形式实域的每个元是全正的. 我们有下述的一般准则

定理 10. 设Φ是一个特征$\neq 2$ 的域. 则Φ的元 $\rho(\neq 0)$在Φ内是全正的当且仅当ρ是Φ的元之平方和.

证 如果 $0 \neq \rho = \Sigma\alpha_i^2$, 则显然在$\Phi$的每个序中有 $\rho > 0$. 反之,设$\rho \neq 0$在Φ内不是平方和,令Ω是Φ的一个代数闭包, 并考虑 Ω/Φ 的子域E的集族,在其中ρ不是平方和.该集族包含Φ且为归纳集; 因此它含有一个极大元 P. 于是P是形式实域;否则,§1的引理表明P的每个元是平方和,但已知ρ在P内不是平方和.故P能序化. 其次,注意到$-\rho$ 在P内是一个平方元素. 否则,可得域 $\mathrm{P}(\sqrt{-\rho})$在Ω内,而且此域真正包含 P. 因此在此域中,必须有 $\rho = \Sigma(\xi_i + \eta_i\sqrt{-\rho})^2$,$\xi_i,\eta_i$ 在P内. 这就得到$\rho = \Sigma\xi_i^2 - \rho\Sigma\eta_i^2 - 2(\Sigma\xi_i\eta_i\sqrt{-\rho})$. 由此得 $\Sigma\xi_i\eta_i = 0$,那么 $\rho(1 + \Sigma\eta_i^2) = \Sigma\xi_i^2$. 故由P的形式实性得 $1 + \Sigma\eta_i^2 \neq 0$;故由§1的引理得: 在P内 $\rho = (\Sigma\xi_i^2)(1 + \Sigma\eta_i^2)^{-1}$是平方和,这矛盾于P的选择,因此我们有$-\rho = \beta^2$,$\beta \in \mathrm{P}$. 由此得出在P的每种序里$-\rho > 0$,$\rho < 0$. 因为P可以序化, 故$\Phi$中的诱导序给出了$\Phi$的一个序, 在此序中 $\rho < 0$. 因此ρ不是全正的.

由这个准则和在前面关于有理数域的有限维扩张中序的形式所得到的结果容易推得下述的

定理 11(希尔伯特-兰道). 设Γ是有理数域的有限维扩张域,$\tau_1,\tau_2,\cdots,\tau_r(r \geq 0)$ 是 Γ/R_0 到实代数数域内不同的同构,则Γ的元$\rho \neq 0$是Γ内元的平方和当且仅当 $\rho^{\tau_i} > 0$, 对 $i = 1, 2, \cdots, r$.

习 题 50

1. 设Φ是一个有序域，Λ是Φ上的一个形式实域．设ρ是Λ的一个元，它不能写为形式

(10) $$\Sigma\beta_i\xi_i^2,\quad \beta_i\geqslant 0,\quad \beta_i\in\Phi,$$

ξ_i属于较大的域．证明存在Λ的一个代数扩张P，ρ在P中不能写成（10）的形式（$\xi_i\in$ P），但ρ在P的每个真代数扩张P′中有这个形式．证明Φ的每个正元是P的平方元，因此ρ在任一P′$\supset$P中是一个平方和，P′在P上是代数的．证明P是实闭域，而且P中的序是Φ中序的一个扩张．证明对于P的序有$\rho<0$．由此证明下述定理：Λ的一个元ρ在Λ中有形式(10)的充分必要条件是：对Λ的每个扩张Φ的序来说，都有$\rho\geqslant 0$．

2. 设Φ是一个有序域，Δ是Φ的实闭包，Γ是Φ的有限维扩张．证明下述定理9的推广：如果r是Γ/Φ到Δ/Φ内的同构的个数，则r是把Φ的序扩张成Γ的序之方法的个数．

6. 正定有理函数 希尔伯特在1900年巴黎数学家代表大会上的致词中所提出的问题之一如下：设Q是n个变量的有理系数的有理函数，它对于一切使Q有定义的实的$(\xi_1,\cdots,\xi_n)$都有$Q(\xi_1,\cdots,\xi_n)\geqslant 0$．问：$Q$必须是有理系数的有理函数的平方和吗[1]？有理系数的有理函数是指一个映射$(\xi_1,\cdots,\xi_n)\to Q(\xi_1,\cdots,\xi_n)$，其中$Q(x_1,\cdots,x_n)$是未定元$x_i$的具有理系数的有理表达式．$Q$的定义域是使$Q(x_1,\cdots,x_n)$的分母不为零的实的$n$元组$(\xi_1,\cdots,\xi_n)$的集．1927年阿廷对希尔伯特问题给出了一个肯定的回答，并证明了下述更强的结果．

定理 12（阿廷）． 设Φ是一个实数的域(即通常实数域的一个子域)，有唯一的序，并设Q为系数在Φ中的有理函数，它是有理正定的，即对所有使Q有定义的有理数组(ξ_i)有$Q(\xi_1,\cdots,\xi_n)\geqslant 0$．则$Q$是系数在$\Phi$中的有理函数的平方和．

满足条件的域Φ之例子是：有理数域，任一个实数的实闭子域，一切实数的域．如果我们取Φ是这些域的第一个，则阿廷定理

---

1) 这是著名的希尔伯特第17问题．参看D. Hilbert,《数学问题》,载Göttinger Nachrichten, 1900, p. 284 或 Gesammelte Abhandlungen, Vol. 3, p. 317．——著者注．

给出了一个较希尔伯特提出的还要强的结果．设Φ如定理所设，考虑域 $\Phi(x_i)=\Phi(x_1,x_2,\cdots,x_n)$，其中 x_i 为未定元，系数在Φ中．此域是形式实域（§1，习题的第4题）．根据定理10，在 $\Phi(x_i)$ 中 $Q(x_1,\cdots,x_n)\neq 0$ 是此域的元的平方和当且仅当对 $\Phi(x_i)$ 的每种序都有 $Q>0$．因此，如果我们能证明，"若 $Q\neq 0$ 是有理正定的，则对 $\Phi(x_i)$ 的每种序均有 $Q>0$"就能推出定理12．这可由下述定理推出．

定理 13. 设Φ是一个实数的域，$\Phi(x_i)=\Phi(x_1,\cdots,x_n)$为$n$个未定元 x_i 的系数在Φ中的有理式的域，并设给定 $\Phi(x_i)$ 一个序，它是Φ作为实数域的一个子域的序的扩张．设 $f_1(x_1,\cdots,x_n),\cdots,f_k(x_1,\cdots,x_n)$ 是 $\Phi(x_i)$ 中元的一个有限集，则存在一个有理n元组 $(a_1,\cdots,a_n)$ 使得对于每个 $j,1\leqslant j\leqslant k,f_j(a_1,\cdots,a_n)$ 在以下意义下有相同的符号：$f_j(a_1,\cdots,a_n)\gtreqless 0$ 根据 $\Phi(x_i)$ 中给定的序 $f_j\gtreqless 0$ 而定．

假设此结果成立并设Φ如定理12所示．设$Q\neq 0$是 $\Phi(x_i)$ 的一个元，它不是 $\Phi(x_i)$ 中的平方和．则存在 $\Phi(x_i)$ 的一个序对此序有 $Q<0$．因为Φ仅有一个序，则 $\Phi(x_i)$ 的序是Φ的序的扩张．故定理13给出一个集 (a_i)，a_i 为有理数，使得 $Q(a_i)<0$．则Q不是有理正定的．因此我们知道，如果Q是有理正定的，则它是 $\Phi(x_i)$ 的元的平方和，而这就是阿廷定理．

在作了某些必要的准备工作之后，我们将对 x_i 的个数n用归纳法来证明定理13：如果 $n=0$，此结果是显然的，因为此时 $\Phi(x_i)=\Phi$，即此函数刚好是常量函数．剩下来的是证明归纳步骤，于是我们假定结果对 $\Phi(x_1,\cdots,x_n)$ 是对的，要证明结果对 $\Phi(x_1,\cdots,x_n,y)$ 也成立，其中y是一个另外的未定元．又将看到，在本质上，考虑系数在 $\Phi(x_i)$由y的多项式就足够了．设 $F_1(x_i,y),\cdots,F_k(x_i,y)\in\Phi(x_i)[y]$，则我们称含$y$的多项式的这个集的性质P为可有理特殊化的，如果在 $\Phi(x_i)$ 内存在元 $\phi_1(x_i),\cdots,\phi_h(x_i)$ 的集使得当 $(a_1,\cdots,a_n)$ 是任一个有理n元组，对此n元组 $\phi_1,\cdots,\phi_h$ 是有定义的，而且 $\phi_l(a_i)$，$1\leqslant l\leqslant h$，与 ϕ_l 有相同

的符号(对于 $\Phi(x_i)$ 中某一给定的序),则所有 $F_j(x_i, y)$ 的系数在 $(a_1, \cdots, a_n)$ 上是有定义的，而且多项式 $F_1(a_i, y), \cdots, F_k(a_i, y)$ 有性质 P. 关于可特殊化的性质需要两个结果，我们将它们表述为引理.

引理 1. $F(x_i, y) = y^m + \varphi_1(x_i) y^{m-1} + \cdots + \varphi_m(x_i)$ 在 $\Phi(x_i)$ 的实闭包中恰有 r 个根的这一性质是可有理特殊化的.

证 我们设 Φ 为实数域的一个子域，而且 Φ 被实数的域的序所序化. 后者中关于 Φ 是代数元的元所成的子域是 Φ 的一个实闭包(定理 6 的推论和§4 的习题的第 2 题). 此引理断言在 $\Phi(x_i)$ 中存在 $\phi_1, \phi_2, \cdots, \phi_h$ 使得: 如果 $(a_1, \cdots, a_n)$ 是任一个有理 n 元组使得每个 ϕ_l 在 $(a_1, \cdots, a_n)$ 上有定义,而且 $\phi_l(a_1, \cdots, a_n)$ 与 ϕ_l 有相同的符号,则 $F(a_i, y)$是有定义的,而且它的实根个数(或者在Δ中根的个数) 是 r. 设 $F_0 = F(x_i, y)$, $F_1, \cdots, F_s$ 为对 $F(x_i, y)$ 的标准序列(如公式(7)所示). 如果 $(a_1, \cdots, a_n)$ 是有理 n 元组,对于$(a_1, \cdots, a_n)$, F_j 的非零系数和如同(7)中的商 Q_j 是有意义的,并在Φ中有非零值,则 $F_0(a_i, y), \cdots, F_s(a_i, y)$ 对于 $F(a_i, y) = F_0(a_i, y)$是标准序列. 设 $\eta(x_i) = \sum_{j=1}^{m} \varphi_j(x_i)^2 + (m+1)$,则我们已知(p.   )$F(x_i, y)$ 在 $\Phi(x_i)$ 的实闭包中的 r 个根落在区间$(-\eta, \eta)$内. 由斯图姆定理知，两个序列 $F_0(x_i, -\eta)$, $F_1(x_i, -\eta), \cdots, F_s(x_i, -\eta)$ 和 $F_0(x_i, \eta)$, $F_1(x_i, \eta), \cdots, F_s(x_0, \eta)$ 之间的变号数的差是 r. 现设$\{\phi_1(x_i), \cdots, \phi_h(x_i)\}$是 $\Phi(x_i)$的元的集，它是由 F 的标准序列的系数和这序列的商 Q_j 的系数以及元 $F_j(x_i, -\eta(x_1, \cdots, x_n)), F_j(x_i, \eta(x_1, \cdots, x_n)), 0 \leqslant j \leqslant s$ 所组成. 则由斯图姆定理显然有: 如果 $(a_1, \cdots, a_n)$ 是有理 n 元组,使得每个 ϕ 在 $(a_1, \cdots, a_n)$上有定义,而且每个 $\phi_l(a_1, \cdots, a_n)$ 与 ϕ_l 有相同的符号, 则 $F(a_i, y)$ 是有定义的，而且在Δ的 $(-\eta(a_1, \cdots, a_n), \eta(a_1, \cdots, a_n))$ 中恰有 r 个根. 如果我们注意到关于根的界的结果,就知道 $F(a_i, y)$在指出的区间以外没有根，因此 r 是 $F(a_i, y)$ 的实根的个数.

引理 2. 设 $\{F_1(x_i,y),\ \cdots,F_t(x_i,y)\}$ 是属于 $\Phi(x_i)[y]$ 的多项式(不一定不同)序列．设它们的首项系数为 1，则 $F_i(x_i,y)$ 在 $\Phi(x_i)$ 的实闭包内有一个根 ρ_i 而且 $\rho_1<\rho_2<\cdots<\rho_t$ 这个性质是可有理特殊化的．

证 元 ρ_k 和 $(\rho_{j+1}-\rho_j)^{1/2}$, $1\leqslant j\leqslant t-1$, 都含于P中，而且这些元生成 $\Phi(x_i)$ 的一个有限扩张域 Λ，它有一个本原元 θ，设 $g(x_i,y)$是 θ 关于 $\Phi(x_i)$ 的最小多项式．我们有 $\rho_k=\varphi_k(x_i,\theta)$, $(\rho_{j+1}-\rho_j)^{1/2}=\sigma_j(x_i,\theta)$,其中 $\varphi_k(x_i,y),\sigma_j(x_i,y)\in\Phi(x_i)[y]$. 因为 $F_k(x_i,\rho_k)=0, F_k(x_i,\varphi_k(x_{i'},y))$有 θ 作为根,而且由于 $g(x_i,y)$ 是 θ 的最小多项式,我们有

(11) $$F_k(x_i,\varphi_k(x_{i'},y))=G_k(x_i,y)g(x_i,y),1\leqslant k\leqslant t.$$

类似地,关系式 $\rho_{j+1}-\rho_j=\sigma_j(x_i,\theta)^2$ 或者 $\varphi_{j+1}(x_i,\theta)-\varphi_j(x_i,\theta)=\sigma_j(x_i,\theta)^2$ 给出 $\Phi(x_i)[y]$ 中的关系

(12) $$\varphi_{j+1}(x_i,y)-\varphi_j(x_i,y)-\sigma_j(x_i,y)^2 =H_i(x_i,y)g(x_i,y),\qquad 1\leqslant j\leqslant t-1.$$

由于 $\sigma_j(x_i,\ \theta)\neq 0$，它在 Λ 中有一个逆 $\tau_j(x_i,\ \theta)$，那么我们在 $\Phi(x_i)[y]$ 中有以下形式的关系式:

(13) $$\sigma_j(x_i,y)\tau_j(x_i,y)-1=k_j(x_i,y)g(x_i,y).$$

设 $\{\phi_l(x_1,\cdots,x_n)\}$ 是 $\Phi(x_i)$ 的下述元的有限集,它包括$F_k(x_i,y)$ 的系数,所有出现在(11),(12)和(13)中的 y 的多项式的系数以及引理 1 所给出的保证 $g(a_i,y)$ 有实根 γ 的元的集．而且，如果选择 a_i 使每个 $\phi_l(a_i)$ 是有定义的,则出现在(11),(12)和(13)中的每个多项式把 y 代以 γ 是允许的． 在 (11) 中代入 $y=\gamma$ 知道 $F_k(a_i,y)$ 有根 $\beta_k\equiv\varphi_k(a_i,\gamma)$,在(12)中代入 $y=\gamma$ 得 $\beta_{j+1}-\beta_j=\varphi_{j+1}(a_i,\gamma)-\varphi_j(a_i,\gamma)=\sigma_j(a_i,\gamma)^2\geqslant 0$. 由(13),得$\sigma_j(a_i,\gamma)\tau_j(a_i,\gamma)=1$. 因此 $\sigma_j(a_i,\gamma)\neq 0$ 且 $\beta_{j+1}>\beta_j$. 故如所要求那样 $F_j(a_i,y)$ 有实根 β_j,而且 $\beta_1<\beta_2<\cdots<\beta_t$.

现在我们可以给出

定理13的证明. 正如在前面所看到的，只要证明下述结果就够了：如果定理对 $\Phi(x_1,\cdots,x_n)$成立,则定理对 $\Phi(x_1,\cdots,x_n,$

y) 成立,这里 y 是另外一个未定元. 设 P′ 是有序域 $\Phi(x_i, y)$ 的一个实闭包, P 是含于 P′ 的 $\Phi(x_i)$ 的实闭包. 给定 $\Phi(x_i,y)$ 的元 $F(x_i,y)$ 的一个有限集,我们要证明可以选择有理数 a_i 和 b 使得 $F(a_i,b)$ 是有定义的而且与 $F(x_i, y)$ 在 P′ 的序中有相同的符号,此点对给定集的每个 F 都成立. 可以记 $F = \varphi(x_1,\cdots,x_n)$ $P_1(x_i,y)^{e_1}\cdots P_h(x_i, y)^{e_h}$, 而 $\varphi(x_1,\cdots,x_n)\in\Phi(x_i)$, e_j 是整数, $P_j(x_i,y)$ 在 $\Phi(x_i)[y]$ 中不可约,其首项系数为 1,而且 $P_j(x_i,y)$ 是不同的. 如果 a_i,b 有性质: $\varphi(a_1,\cdots,a_n)$, $P_j(a_i,b)$ 是有定义的,而且与 φ 和 P_j 有相同的符号, $1\leqslant j\leqslant h$, 则 $F(a_1,\cdots, a_n,b)$ 是有定义的, 而且与 F 有相同的符号. 这一陈述表明我们也可以假设给定的集可以由元 $\varphi\in\Phi(x_i)$ 和 $F\in\Phi(x_i)[y]$ 所组成使得每个 F 在 $\Phi(x_i)[y]$ 中不可约, 且首项系数为 1. 设 $\rho_1<\rho_2<\cdots<\rho_t$ 是给定的 y 的多项式集 $\{F\}$ 在 P 中的根. 可作一序列 $F_1,F_2,\cdots,F_t$,它的项取自$\{F\}$, 并使得 ρ_j 是 F_j 的根. 因为 F 是不可约的,而且域的特征为 0, 故 F 的根是不同的. 又不同的 F 是互变的. 因此,如果 $G(x_i,y)$ 是不同的 F 的乘积, 则 G 有不同的根. 由引理 1,可以在 $\Phi(x_i)$ 中找到元 $\phi_1,\cdots,\phi_h$ 使得,如果 $a_1,\cdots,a_n$ 是有理数, 而且每个 ϕ_l 在 $(a_1,\cdots, a_n)$ 上是有定义的, $\phi_l(a_1,\cdots,a_n)$与 ϕ_l 有相同的符号, $1\leqslant l\leqslant h$, 则 $G(a_i,y)$ 是有定义的并有 t 个实根. 由引理 2,我们有元 $\phi_{h+1},\cdots,\phi_k$ 使得,如果诸 a 是有理数, $\phi_m(a_1,\cdots,a_n)$ 是有定义的而且与 ϕ_m 有相同的符号, $h+1\leqslant m\leqslant k$,则 $F_j(a_i,y)$ 是有定义的并有一实根 β_j 使得 $\beta_1<\beta_2<\cdots<\beta_t$. 现在我们在已经给出的诸 ϕ 上添加原给定集的一切元 φ 以及 $G(x_i,y)$ 的判别式 δ, 由于 G 有不同的根, δ 是异于零的. 由归纳法假设,我们可以选择有理数 a_i 使得对诸 ϕ, 诸 φ 和 δ 满足所给的一切条件. 于是在 $P[y]$ 中有因式分解

$$(14)\qquad F_j(x_i,y) = (y-\rho_{j_1})(y-\rho_{j_2})\cdots (y-\rho_{j_{t_j}})Q_1(y)\cdots Q_{s_j}(y),$$

其中诸 Q 是首项系数为 1 的二次不可约多项式, $\{j_1,j_2,\cdots, j_{tj}\}$不同且为$\{1,2,\cdots,t\}$的一个子集, a 的选择保证了在实数的域中有

(15) $$F_j(a_i,y)=(y-\beta_{i_1})(y-\beta_{i_2})\cdots(y-\beta_{i_{t_j}})S_1(y)\cdots S_{s_j}(y),$$

其中 S 都是首项系数为 1 的不可约二次式. 因 y 在 $\Phi(x_i)$ 上是超越的而 ρ_l 在此域上是代数的,显然 y 含于 P′ 内下述开区间中的一个: $(-\infty,\rho_1),(\rho_1,\rho_2),\cdots,(\rho_{t-1},\rho_t),(\rho_t,\infty)$. 我们又已知道系数在一个实闭域内、首项系数为 1 的一个二次不可约多项式有形式 $(y-\gamma)^2+\delta^2,\delta\neq 0$ (参看(3)). 由此得在 P′ 中每个 $Q(y)>0$, 而且对任意实数 b, 对(15)中的诸 S 有 $S(b)>0$. 于是由(14)和(15)推出: 如果 y 在序列 $(-\infty,\rho_1),(\rho_1,\rho_2),\cdots,(\rho_t,\infty)$ 的第 k 个区间, b 是含于序列$(-\infty,\beta_1),(\beta_1,\beta_2),\cdots,(\beta_t,\infty)$的第 k 个区间中的任一实数, 则 $F_j(a_i,b)$ 和 $F_j(x_i,y)$ 有相同的符号,而且对每个 j 均成立. 由实数域的阿基米得性质,每个开的实区间含有一个有理数, 故可选择有理数 b 使对所有的 $j,F_j(a_i,b)$ 与 $F_j(x_i,y)$ 有相同的符号. 证毕.

注. 自然有人会问,如果域 Φ 如阿廷定理所要求的,则对系数在 Φ 中的多项式是否有类似于阿廷的结果成立. 利用阿廷定理我们能用下述方法把此问题公式化: 设 $\mathrm{P}(x_1,\cdots,x_n)\in\Phi[x_1,\cdots,x_n]$ 使得 $\mathrm{P}=\Sigma R_i(x_1,\cdots,x_n)^2$, 其中 R_i 是诸 x 的系数在 Φ 中的有理(表达)式, 能否由此推出 $\mathrm{P}=\Sigma\mathrm{P}_i(x_1,\cdots,x_n)^2$, $\mathrm{P}_i\in\Phi[x_1,\cdots,x_n]$. 阿廷已证明若 $n=1$, Φ 是任何实数的域时这是正确的. 另一方面,若干属于希尔伯特的例子表明对 $n\geq 2$,纵然 Φ 为实数域此结果也是不正确的.

习 题 51

1. 设 Φ 是一个有序域,$\Phi(x_1,\cdots,x_n)$是 Φ 上未定元 $x_1,\cdots,x_n$ 的有理表达式的域. 假设$Q\in\Phi(x_i)$ 对 Φ 的实闭包Δ中的一切使 $Q(\xi_1,\cdots,\xi_n)$ 有定义的 ξ_i,满足 $Q(\xi_1,\cdots,\xi_n)\geqslant 0$,证明 $Q=\Sigma\beta_iF_i(x_1,\cdots,x_n)^2$,其中 β_i 是 Φ 的非负元,$F_i\in\Phi(x_i)$.(提示: 参看§5 习题的第 1 题和证明定理 13 的适当类比.)

7. 斯图姆定理的形式化. 结式 在下面的少数几节里, 我们要发展一种由塔尔斯基和赛登堡创建的算法,它是用来判别(含多个变量的) 多项式方程和不等式的有限组在一个实闭域内的可解

性的.最终的判别法(定理 16)将由在所给组的系数中检验一个多项式方程和不等式的有限组构成. 本节我们将首先考虑用这种方法将斯图姆定理再公式化,我们还将发展一种基于结式的消去法,这对以后是重要的.

为了得到斯图姆定理的形式说法,从环 $\mathfrak{A}[x]$ 开始是方便的,这里 $\mathfrak{A}=R_0[t_1,\cdots,t_r]$, x 和 t_i 是未定元, R_0 是有理数域. 设 $F(t_1,\cdots,t_r;x)\in\mathfrak{A}[x]$,那么 $F(t_i;x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$, 而 $a_i\in\mathfrak{A}$, $a_n\neq 0$. 如果把 t_i 特殊化取 $t_i=\tau_i\in\Phi$, 则得到多项式 $f(x)=F(\tau_i;x)\in\Phi[x]$,其中 $\deg f(x)\leqslant n$. 于是我们将得到若干序列 $E:\{F_0(t_i;x),F_1(t_i;x),\cdots,F_s(t_i;x)\}$ 使得对任何 τ_i, $1\leqslant i\leqslant r$, 在 Φ 中存在这些序列 E 中的一个使得此特殊序列 $\{F_0(\tau_i;x),F_1(\tau_i;x),\cdots,F_s(\tau_i;x)\}$ 实质上就是 $f(x)$ 的标准斯图姆序列(7).

我们选择 $F_0(t_i;x)$ 为任一个多项式 $a_mx^m+a_{m-1}x^{m-1}+\cdots+a_0$, $a_m\neq 0$, $m\leqslant n$, 它是去掉 $F(t_i;x)$ 的开始几项 $a_nx^n+\cdots+a_{m+1}x^{m+1}$ 而得到的. 接着我们取 $F_1(t_i;x)=F_0'(t_i;x)$ 即 F_0 作为含 x 的多项式时之形式导数. 假设我们已经定义了 F_0, $F_1,\cdots,F_k$. 如果 $F_k=0$,则我们得到了序列 $F_0,F_1,\cdots,F_s=F_{k-1}$,就不往下做了. 否则, 设 $F_{k-1}=b_px^p+\cdots+b_0$, $F_k=c_qx^q+\cdots+c_0$,其中 $b_p\neq 0,c_q\neq 0$, 而且 $p>q$. 通常的除法过程表明我们可以在 $\mathfrak{A}[x]$ 中找到多项式 $Q(x)$, $R(x)$ 使得 $c_q^{p-q+1}F_{k-1}=QF_k-R$,而 $\deg_xR(t_i;x)<\deg_xF_k(t_i;x)$. 对我们来说,用最小的偶整数 $e\geqslant p-q+1$ 来替 $p-q+1$ 更为方便. 因此,改变记号,记 $c_q^eF_{k-1}=QF_k-R$, 并称 Q 和 R 为用 F_k 除 F_{k-1} 所得的**商**和**余式**. 显然这些是唯一的. 现在我们取 F_{k+1} 是 R 或者可以由 R 出发所得的一个多项式,它类似于从 $F(t_i;x)$ 得到 $F_0(t_i;x)$,由去掉开头的若干项而得的.用这种方法得到的序列 $\{F_0,F_1,\cdots,F_s\}$ 将称为对 $F(t_i;x)$ 的**一般标准序列**. 显然其个数是有限的.

设 $E:\{F_0,F_1,\cdots,F_s\}$ 是对于 F 的一般标准序列中的一个,

则有 $\mathfrak{A}=R_0[t_i]$ 的两个有限子集 $\delta(E)$ 和 $\lambda(E)$ 与 E 有关联. 集 $\delta(E)$ 是由组成序列时去掉那些项的系数的集. 因此, $\delta(E)$ 是由 $F(t_i;x)-F_0(t_i;x)$ 中 (x 的各个幂)的系数和上述的 $R-F_{k+1}(k\geqslant 1)$ 的系数所组成的. 我们令 $\lambda(E)$ 是由序列中 F_i 的开头项系数所组成的.

现令 $\tau_i\in\Phi, 1\leqslant i\leqslant r$, 并考虑多项式 $f(x)=F(\tau_i;x)$. 假设 $f(x)\neq 0$, $\deg f(x)=m\leqslant n$, 则我们取 $F_0(t_i;x)=a_mx^m+\cdots+a_0$ 并有 $F_0(\tau_i;x)=f(x), a_m(\tau_i)\neq 0$. 由条件 $F_0(\tau_i;x)=f(x)$ 得 $a_n(\tau_i)=\cdots=a_{m+1}(\tau_i)=0$. 用归纳法易知对于 F 存在一个一般标准序列 $\{F_0,F_1,\cdots,F_s\}$ 使得: 如果 l_k 是 F_k 的开头项系数, 则

$$
\begin{aligned}
&l_k(\tau_i)\neq 0, 0\leqslant k\leqslant s,\\
(16)\qquad &F_0(\tau_i;x)=f(x),\\
&l_k(\tau_i)^{e_k}F_{k-1}(\tau_i;x)=F_k(\tau_i;x)Q_k(\tau_i;x)\\
&\quad -F_{k+1}(\tau_i;x),
\end{aligned}
$$

其中 $0\leqslant k\leqslant s, F_{s+1}=0, e_k$ 是偶整数, Q_k 是用 F_k 除 F_{k-1} 的商. 因为 $F_0(\tau_i;x)=f(x), F_1(\tau_1;x)=f'(x), l_k(\tau_i)^{e_k}>0$, 而 $F_k(\tau_i;x)$ 的次数是下降的, 显然 $\{F_0(\tau_i;x),F_1(\tau_i;x),\cdots,F_s(\tau_i;x)\}$ 的项与 $f(x)$ 的标准序列(7) 的这些项相差一个 Φ 中的正因子. 因此在应用斯图姆定理的时候序列 $\{F_0(\tau_i;x),\cdots\}$ 可用来代替标准序列.

于是我们将使在定理中给出的条件形式化, 这是通过考察由下述类型的关系所组成的方程和不等式组的有限集族实现的:

$$
\begin{aligned}
(17)\qquad &F_k(t_i;y)F_l(t_i;y)<0,\\
&F_{k+1}(t_i;y)=\cdots=F_{l-1}(t_i;y)=0, k<l,\\
&F_p(t_i;z)F_q(t_i;z)>0,\\
&F_{p+1}(t_i;z)=\cdots=F_{q-1}(t_i;z)=0, p<q,
\end{aligned}
$$

其中 y 和 z 是未定元, 并要求出现在上述两种关系集中的数对 $(k,l),\cdots,(p,q),\cdots$ 如果 $\varepsilon_k=0,1,-1, \eta=0, 1,-1$ 满足相同的条件, 即 $\varepsilon_k\varepsilon_l<0$, $\varepsilon_{k+1}=\cdots=\varepsilon_{l-1}=0$, $\cdots$, $\eta_p\eta_q>0$,

$\eta_{p+1}=\cdots=\eta_{q-1}=0$, $\cdots$, 则 $\{\varepsilon_0,\varepsilon_1,\cdots,\varepsilon_r\}$ 的变号数超过 $\{\eta_0,\eta_1,\cdots,\eta_r\}$ 的变号数. 现令 (β,γ) 是 Φ 中的一个区间, $\beta<\gamma$, 使得 $f(\beta)\neq 0, f(\gamma)\neq 0$. 则从斯图姆定理显然有: $f(x)$ 在 (β,γ) 中有一个根当且仅当 $t_i=\tau_i$, $y=\beta$, $z=\gamma$ 满足一组关系式(17).

如果我们考虑所有一般序列 E 并注意到 (16) 是等价于条件: 对一切 $l\in\lambda(E)$ 和 $d\in\delta(E)$ 有 $l(\tau_i)\neq 0, d(\tau_i)=0$, 我们看到(16)和(17)给出条件$\{G_1,G_2,\cdots,G_h\}$的一个有限集族, 其中每个 G_j 是有理系数多项式方程和不等式的一个有限集, 使得 $f(x)$ 在 (β,γ)内有根当且仅当 $t_i=\tau_i, y=\beta$, $z=\gamma$ 满足某一组 G_j 的所有条件.

现设 $f(x)=\alpha_m x^m+\alpha_{m-1}x^{m-1}+\cdots+\alpha_0$, 而 $\alpha_m\neq 0$. 则我们知道 $f(x)$ 在 Φ 中的所有根含于区间 $(-\eta,\eta)$, 其中 $\eta=m+1+\sum_0^{m-1}\alpha_j^2\alpha_m^{-2}$. 我们有 $F_0(t_i;x)=a_m x^m+a_{m-1}x^{m-1}+\cdots+a_0$, 其中 $a_m=a_m(t_1,\cdots,t_r)\neq 0$. 如果在 $F_k(t_i;y)$ 中代入 $y=-(m+1)-\sum_0^{m-1}a_j^2a_m^{-2}$, 在 $F_k(t_i;z)$ 中代入 $z=m+1+\sum_0^{m-1}a_j^2a_m^{-2}$, 并乘以 a_m 的适当的偶数幂去掉分式, 就得到只含 t_i 的类似于(17)的多项式. 由此可见我们得到了一个有限集族$\{G_1, G_2,\cdots, G_h\}$, 其中每个 G_j 是有理系数且仅含 t_i 的多项式方程和不等式的一个有限组, 使得"$f(x)$ 在Φ中有一个根"这个命题等价于"当 $t_i=\tau_i$ 时有某一组 G_j 成立".

下面, 我们将考虑两个多项式有正次数公因式存在的古典行列式准则. 考虑 $\Phi[x]$ 中的两个多项式 $f(x)=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\cdots+\alpha_0$, $g(x)=\beta_m x^m+\beta_{m-1}x^{m-1}+\cdots+\beta_0$, Φ 为任一个域. 设 $m>0, n>0$, 但我们允许 $\alpha_n=0$ 或者 $\beta_m=0$. 我们要的结果如下:

定理 14. 设 $f(x)=\alpha_n x^n+\alpha_{n-1}x^{n-1}+\cdots+\alpha_0, g(x)=$

$\beta_m x^m + \beta_{m-1}x^{m-1} + \cdots + \beta_0$，其中 $m,n > 0$，并令

$$
(18)\qquad R(f,g) = \left|\begin{array}{cccccc}
\alpha_n & \alpha_{n-1}\cdots & \alpha_0 & & & \\
 & \alpha_n & \alpha_{n-1}\cdots\alpha_0 & & & \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & & & \alpha_n & \alpha_{n-1}\cdots\alpha_0 & \\
\beta_m & \beta_{m-1}\cdots\cdots\beta_0 & & & & \\
 & \beta_m & \beta_{m-1}\cdots\beta_0 & & & \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & & & \beta_m & \beta_{m-1}\cdots\beta_0 &
\end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\ \\ \\ \\ \end{array}\right\} m\text{行} \\ \left.\begin{array}{l}\\ \\ \\ \\ \end{array}\right\} n\text{行}\end{array}
$$

则 $R(f,g)=0$ 当且仅当 $\alpha_n = 0 = \beta_m$ 或者 $f(x)$ 和 $g(x)$ 有关于 x 的正次数的公因式。

证　如果 $\alpha_n = 0 = \beta_m$，则行列式的第一列是 0．因此 $R(f,g) = 0$．下面设 $f(x)$ 和 $g(x)$ 有正次数的公因式 $h(x)$ 又有 $\alpha_n \neq 0$ 或者 $\beta_m \neq 0$，则 $f(x) = f_1(x)h(x)$，$g(x) = g_1(x)h(x)$，并有 $f_1(x) \neq 0$ 或者 $g_1(x) \neq 0$，根据 $\alpha_n \neq 0$ 或者 $\beta_m \neq 0$ 而定．由对称性，可设 $\alpha_n \neq 0$，$f_1(x) \neq 0$，则有 $f(x)g_1(x) = g(x)f_1(x)$，$f(x)=f_1(x)h(x) \neq 0$．如果 $\deg h(x) = r$，则 $\deg f_1 = n - r$．如果 $g(x) = 0$，则 $g_1(x) = 0$．否则由关系式 $f(x)\ g_1(x) = g(x)\ f_1(x)$ 得出 $\deg g_1(x) \leqslant m - r$．因此可记 $f_1(x) = -\gamma_{n-1}x^{n-1} - \gamma_{n-2}x^{n-2} - \cdots - \gamma_0$，$g_1(x) = \delta_{m-1}x^{m-1} + \delta_{m-2}x^{m-2} + \cdots + \delta_0$，使得有

$$
(19)\qquad \begin{aligned}&(\alpha_n x^n + \cdots + \alpha_0)(\delta_{m-1}x^{m-1} + \cdots + \delta_0)\\ &+ (\beta_m x^m + \cdots + \beta_0)(\gamma_{n-1}x^{n-1} + \cdots + \gamma_0) = 0.\end{aligned}
$$

如果我们使(19)中 $x^{m+n-1}, x^{m+n-2}, \cdots, 1$ 的系数等于 0，得下述方程：

$$
(20)\qquad \begin{aligned}\alpha_n\delta_{m-1} + \beta_m\gamma_{n-1} &= 0\\ \alpha_n\delta_{m-2} + \alpha_{n-1}\delta_{m-1} + \beta_m\gamma_{n-2} + \beta_{m-1}\gamma_{n-1} &= 0\\ &\vdots\\ \alpha_0\delta_0 + \beta_0\gamma_0 &= 0.\end{aligned}
$$

我们把(19)看作诸 γ 和 δ 的齐次方程组，诸 γ 和 δ 按下述的顺序

排列：$\delta_{m-1},\delta_{m-2},\cdots,\delta_0,\gamma_{n-1},\cdots,\gamma_0$. 因为诸 γ 不全为 0，故 γ 和 δ 的系数行列式为0. 如果我们取此行列式的转置(此行列式是按所指出的诸 γ 和 δ 的顺序而得到的)，则得(18). 故 $R(f,g)=0$. 反之，设 $R(f,g)=0$，则我们可以通过(20)和(19)逆推得出：存在 $f_1(x),g_1(x)$ 使得 $f(x)g_1(x)=g(x)f_1(x)$，而 $\deg f_1\leqslant n-1$，$\deg g_1\leqslant m-1$，而且或者 $f_1\neq 0$ 或 $g_1\neq 0$. 设 $f_1\neq 0$. 如果 $g_1=0$，则 $g=0,\beta_m=0$，而且要么 $f(x)$ 是 f 和 g 的非零公因式，要么就是 $\alpha_n=0$. 如果 $g_1\neq 0$ 和 $g=0$，则上述的论证也适用. 现在设 $g_1\neq 0$ 和 $g=0$，则由关系式 $f(x)g_1(x)=g(x)f_1(x)$，$f_1\neq 0,g_1\neq 0,g\neq 0$ 推出 $f\neq 0$. 或者 $\alpha_n=0=\beta_m$ 或者可以设 $\alpha_n\neq 0$，这说明 $\deg f(x)=n$. 因为 $\deg f_1(x)\leqslant n-1$，由关系式 $f(x)g_1(x)=g(x)f_1(x)$ 和非零多项式 f,f_1,g,g_1 分解为不可约因式可推出 $f(x)$ 和 $g(x)$ 有正次数的公因式.

我们将称 $R(f,g)$ 为 f 和 g（关于 x）的**结式**. 如果 f 或者 g 的最高项系数不为 0，则 $R(f,g)$ 为零是一个关于 α_i,β_j 的整系数多项式关系，它是与 f 和 g 有一个正次数的公因式这一命题等价的.

习　题　52

1. 证明，如果 $f(x)=x^n+\alpha_{n-1}x^{n-1}+\cdots+\alpha_0$，则 $R(f,f')$ 是 $f(x)$ 的判别式(参考§3.1).

8. 代数曲线的判定法　本节我们将给出决定方程 $f(x,y)=0$ 在一个实闭域中可解性的赛登堡方法，这是奠基于我们即将建立的结果之上的：如果 $f(x,y)=0$ 在 Φ 中有解，则方程 $f(x,y)=0$ 和 $(y-\delta)\dfrac{\partial f}{\partial x}-(x-\gamma)\dfrac{\partial f}{\partial y}=0$ 对 Φ 中的任意 γ 和 δ 在 Φ 中有公共解. 从用来证明此定理的两个引理中，可以弄清楚此定理的几何含义.

引理 1.　设 $f(x,y)\in\Phi[x,y]$，x,y 是未定元，Φ 为一实闭域. 则如果 $f(x,y)=0$ 在 Φ 中有一个解，那么它有一个最靠近

原点的解.

证 我们在数对 (ξ,η) 所成的空间 $\Phi^{(2)}$ 中 $(\xi,\eta\in\Phi)$ 考虑曲线 $C:f(x,y)=0$ 和圆 $x^2+y^2=\gamma^2(\gamma\geqslant 0)$ 的交集. 由我们的假设可推出存在 γ 使这个交不空,而且我们要证明使得 C 在 $\Phi^{(2)}$ 中和 $x^2+y^2=\gamma^2$ 相交的 $\gamma(\geqslant 0)$ 的集 S 有极小值. 考虑多项式 $f(x,y)$ 和系数在 $\Phi(c,x)$ 中 y 的多项式 $x^2+y^2-c^2$, 其中 c 和 x 看作未定元, 并建立这两个多项式的结式 $g(c,\ x)$. 公式 (18) 表明 $g(c,\ x)$ 是一个系数在 Φ 中的 c 和 x 的多项式. 如果 (α,β) 是圆 $x^2+y^2=\gamma^2$ 和曲线 C 的一个交点,则 $f(\alpha,y)$ 和 $y^2+\alpha^2-\gamma^2$ 有一个公因式 $y-\beta$. 因此 $g(\gamma,\alpha)=0$, $g(\gamma,x)$ 有根 $\alpha\in\Phi$. 而且, $-\gamma\leqslant\alpha\leqslant\gamma$. 反之,对 $\gamma\geqslant 0$ 设 $g(\gamma,x)$ 在 Φ 中有一个根 α, $-\gamma\leqslant\alpha\leqslant\gamma$. 由于 $y^2+\alpha^2-\gamma^2$ 中 y 的系数为 1,由定理 14 得, $y^2+\alpha^2-\gamma^2$ 和 $f(\alpha,y)$ 在 $\Phi[y]$ 中有一个公因式. 因为 $y^2+\alpha^2-\gamma^2$ 的因式是 $y\pm\beta$, 而 $\beta=(\gamma^2-\alpha^2)^{1/2}$, 由此得 (α,β) 或者 $(\alpha,\ -\beta)$ 是这两条曲线的交点. 因此我们知道使得 C 和 $x^2+y^2=\gamma^2$ 在 $\Phi^{(2)}$ 相交的 $\gamma(\geqslant 0)$ 的集 S 与使得 $g(\gamma,x)=0$ 有根 $x=\alpha\in\Phi(-\gamma\leqslant\alpha\leqslant\gamma)$ 的 $\gamma(\geqslant 0)$ 的集是相同的. 设 S' 是使得 $g(\gamma,\pm\gamma)\neq 0$ 的 γ 所成的 S 的子集. 对这些 γ,其条件是 $g(\gamma,x)$ 在 $(-\gamma,\gamma)$ 中有一个根. 显然我们可以得到 $g(\gamma,x)$,只要把一个有理系数多项式适当地特殊化使得一个参数特殊化为 γ. 因此可以应用上节得到的结果推得 S' 是由形如 $p(c)=0,q(c)=0,r(c)\gtrless 0$ (其中 p,q,r 为系数在 Φ 中的多项式)的多项式方程和不等式所确定的有限个集的并. 容易看出,这样的集是有限个区间的并,这些区间可以是开的,闭的,半开的,单点集或者延拓至无限的集. 由于使得 $g(\gamma,\ \pm\gamma)=0$ 的 γ 的集或者有限或者一切 $\gamma\geqslant 0$, 显然 S 与 S' 有相同的构造. 现在只要能证明: S 在非负元集中的余集是开区间的并. 结论便可得出;因为,由此推出 S 是有限个闭区间的并,故有一极小元. 于是,令 $\delta\geqslant 0$, $\delta\notin S$,则 $g(\delta,x)=0(-\delta\leqslant x\leqslant\delta)$ 在 Φ 中没有解 x. 记 $g(c,x)=g_0(x)+g_1(x)(c-\delta)+\cdots+g_m(x)(c-\delta)^m$,其

中 $g_i(x)$ 都是 x 的多项式. 则在 $-\delta \leqslant x \leqslant \delta$ 中 $g_0(x) \neq 0$. 于是存在 $\delta' > \delta$ 使得 $-\delta' \leqslant x \leqslant \delta'$ 时有 $g_0(x) \neq 0$. 从而存在 $b > 0, B > 0$ 使得对一切 $x \in [-\delta', \delta']$ 有 $|g_0(x)| \geqslant b$, $|g_i(x)| \leqslant B$(§ 3, 习题的第 3 题). 则如果 $|c-\delta| < \frac{1}{2}$和$|c-\delta| < b/4B$ 与 $x \in [-\delta', \delta]$ 有

$$|g(c,x)| \geqslant |g_0(x)| - |g_1(x)(c-\delta) + \cdots + g_m(x)(c-\delta)^m|$$
$$\geqslant b - 2B|c-\delta| > b - \frac{b}{2} = \frac{b}{2}.$$

由此得每个满足 $\delta'' \leqslant \delta', \delta'' < \delta + \frac{1}{2}, \delta'' < \delta + b/4B$ 的 δ''必含于 S 的余集. 故此余集包含一个包含 δ 的开区间, 证毕.

作为在实数域的经典情况, $f(x,y) = 0$ 上的一个点 (α,β) 称为**单点**, 如果

$$\left(\left(\frac{\partial f}{\partial x}\right)_{(\alpha,\beta)}, \left(\frac{\partial f}{\partial y}\right)_{(\alpha,\beta)}\right) \neq (0,0),$$

则过 (α,β) 的法向量是$\left(\left(\frac{\partial f}{\partial x}\right)_{(\alpha,\beta)}, \left(\frac{\partial f}{\partial y}\right)_{(\alpha,\beta)}\right)$, 而曲线在 (α,β) 的**切线**由方程

$$\left(\frac{\partial f}{\partial x}\right)_{(\alpha,\beta)}(x-\alpha) + \left(\frac{\partial f}{\partial y}\right)_{(\alpha,\beta)}(y-\beta) = 0.$$

确定.

现设 (α,β) 是 $C: f(x,y) = 0$ 上的一点, 且 (α, β) 在 $\Phi^{(2)}$ 中最靠近原点, 我们希望证明 $\beta\left(\frac{\partial f}{\partial x}\right)_{(\alpha,\beta)} - \alpha\left(\frac{\partial f}{\partial y}\right)_{(\alpha,\beta)} = 0$. 如果 $(\alpha,\beta) = (0,0)$ 或 (α, β) 不是一个单点, 这是显然的; 否则, 方程表明联结$(0,0)$与(α,β)的向量和法向量是线性相关的. 因此 C 和中心在原点、半径为$(\alpha^2+\beta^2)^{1/2}$ 的圆在(α, β)点有相同的切线. 如果不是这样, 那么 C 在 (α,β) 的切线包含圆的内点, 然而 C 自已却不含圆的内点. 因此, 结论将由下列引理得出:

引理 2. 设 p 为一个圆和一条曲线 $C: f(x,y)=0, f(x,y)\in\Phi[x,y]$ 的交点(其坐标在 Φ 内). 设 p 是一个单点且 C 在 p 的切线有圆的内点,则 C 自己有圆的内点.

证 取 $p=(0,0)$, C 在 p 点的切线为 x 轴. 则 $f(0,0)=0$ 和 $\left(\frac{\partial f}{\partial x}\right)=0$,而且可以假设 $\left(\frac{\partial f}{\partial y}\right)(0,0)=1$. 圆的中心不在 x 轴上,故可记为 (a, b), $a\neq 0$. 我们有 $f(x, y)=f(0, 0)+\left(\frac{\partial f}{\partial x}\right)_0 x+\left(\frac{\partial f}{\partial y}\right)_0 y+\frac{1}{2!}\left[\left(\frac{\partial^2 f}{\partial x^2}\right)_0 x^2+2\left(\frac{\partial^2 f}{\partial x\partial y}\right)_0 xy+\left(\frac{\partial^2 f}{\partial y^2}\right)_0 y^2\right]+\cdots$,故在考虑了 f 的条件后可以写 $f(x,y)=y(1+h(x,y))+g(x)$,其中 $h(0,0)=0$, $g(x)$ 是 x 的可被 x^2 整除的多项式. 因为 $h(0,0)=0$, 我们可以选择 $\delta>0$ 使得当 $|x|\leqslant\delta$ 和 $|y|\leqslant\delta$ 时 $|h(x,y)|\leqslant\frac{1}{2}$,则 $\frac{1}{2}\leqslant 1+h(x, y)\leqslant\frac{3}{2}$, 并且对所有满足 $|x|\leqslant\delta$ 的 x, $\delta(1+h(x,\delta))$ 在 $\frac{1}{2}\delta$ 和 $\frac{3}{2}\delta$ 之间, 同时 $-\delta(1+h(x, -\delta))$ 在 $-\frac{1}{2}\delta$ 与 $-\frac{3}{2}\delta$ 之间. 因 $g(0)=0$,存在 δ', $0<\delta'\leqslant\delta$ 使得若 $|x|\leqslant\delta'$ 时,则 $f(x,\delta)=\delta(1+h(x,\delta))+g(x)>0$ 和 $f(x,-\delta)<0$. 则对每个 x_0, $|x_0|\leqslant\delta'$ 存在 $y_0\in[-\delta,\delta]$ 使得 $f(x_0,y_0)=0$, 则 $y_0=-g(x_0)(1+h(x_0, y_0))^{-1}$ 且

$$
\begin{aligned}
&(a-x_0)^2+(b-y_0)^2\\
&=(a-x_0)^2+\left(b+\frac{g(x_0)}{1+h(x_0,y_0)}\right)^2\\
&=a^2+b^2-2ax_0+x_0^2+\frac{2bg(x_0)}{1+h(x_0,y_0)}+\frac{(g(x_0))^2}{(1+h(x_0, y_0))^2}.
\end{aligned}
$$

因为 $g(x_0)$ 可被 x_0^2 整除,显然,如果我们取 x_0 充分小使得 $ax_0>0$,则 $(a-x_0)^2+(b-y_0)^2<a^2+b^2$. 因此 (x_0,y_0) 是 C 上的一个点而且在给定的圆内.

于是我们的结论表明，如果 $C: f(x,y)=0$ 在Φ内有解，则在Φ内存在一个解，它也在 $y\frac{\partial f}{\partial x}-x\frac{\partial f}{\partial y}=0$ 内. 如果我们用(γ,δ)代替原点，而 $\gamma,\delta\in\Phi$，则我们用同样的方法知道C和曲线D的交含有 $\Phi^{(2)}$ 的一个点，其中 $D: (y-\delta)\frac{\partial f}{\partial x}-(x-\gamma)\frac{\partial f}{\partial y}=0$.

现在我们将应用此结果去得到决定 $f(x,y)=0$ 在Φ内可解性的赛登堡方法. 首先，我们可以得到 $f(x,y)$ 中y的方幂的系数的最高公因式，并令 $f(x,y)=d(x)f_1(x,y)$，其中 $f_1(x,y)$ 不能被单独一个x的正次数多项式所整除. 显然 $f(x,y)=0$ 在Φ中有解当且仅当 $d(x)=0$ 或者 $f_1(x,y)=0$ 有这样的解，这就将讨论归结为不被单独一个x的正次数多项式整除的多项式. 接着，我们可用通常的欧几里得算法在 $\Phi(x)[y]$ 中求出 $f(x,y)$ 和 $\frac{\partial}{\partial y}f(x,y)$ 的最高公因式. 我们可设此多项式属于 $\Phi[x,y]$ 而且不能被单独一个x的正次数的多项式所整除. 然后可以用这个最高公因式去除而得到多项式 $g(x,y)$，它是 $f(x,y)$ 的一个因式，与 $f(x,y)$ 有相同的不可约因式，且在 $\Phi[x,y]$中没有重因式. 显然，$f(x,y)=0$ 在Φ中可解.

如果我们用g代替f并改变记号仍用f表示，我们就可以假设 $f(x,y)$ 没有正次数的重因式和没有单独一个x的正次数的因式. 由这些条件的第一个推出 $f(x,y)$ 和$\frac{\partial}{\partial y}f(x,y)$ 在 $\Phi(x)[y]$ 里没有含y的正次数公因式.

现考虑多项式 $g(x,y)=y\frac{\partial f}{\partial x}-(x-\gamma)\frac{\partial f}{\partial y}$，其中$\gamma$是$\Phi$的任一元. 我们知道，如果曲线 $C: f(x,y)=0$ 含有 $\Phi^{(2)}$ 的点，则C和 $D: g(x,y)=0$ 的交也含有这样的一个点. 在我们应用此点之前有必要调整一下，即选择一个适当的γ使得C和D的交是

一个有限集．为此我们引进另一个未定元 c 并考察多项式 $g(c;x,y)=y\frac{\partial f}{\partial x}-(x-c)\frac{\partial f}{\partial y}$．设 $R(c;x)$ 是 $f(x,y)$和 $g(c;x,y)$关于 y 的结式（即，把这些多项式看作 y 的多项式）．我们断言 $R(c;x)\neq 0$．否则，对一切 $\gamma, R(\gamma;x)=0$．由定理 14 表明，如果 γ 有此性质，则 $g(\gamma;x,y)$ 和 $f(x,y)$ 在 $\Phi(x)[y]$ 中有公因式，因此在 $\Phi[x, y]$ 中有 y 的正次数的公因式（参看卷 I，中译本 p.116)．所以，如果对所有 $\gamma, R(\gamma:x)=0$，则存在不同的 γ，譬如说 γ_1 和 γ_2，使得 $f(x,y), g(\gamma_1;x,y)$ 和 $g(\gamma_2;x,y)$ 三者都有一个含 y 的正次数公因式，这可由下列事实得出：在相伴的意义下 $f(x,y)$ 在 $\Phi(x)[y]$ 内仅有有限多个不同的因式．于是我们可断定 $f(x, y)$ 和 $(\gamma_1-\gamma_2)\frac{\partial}{\partial y}f(x, y)=g(\gamma_1;x,y)-g(\gamma_2;x, y)$ 有一个含 y 的正次数公因式，这与 $f(x,y)$ 和 $\frac{\partial}{\partial y}f(x,y)$ 没有这样的公因式相矛盾．这就证明了 $R(c;x)\neq 0$．

于是我们可以选取 $\gamma\in\Phi$ 使得 $R(x)\equiv R(\gamma; x)\neq 0$．令 $g(x,y)=g(\gamma;x,y)$，则 $f(x,y)$ 和 $g(x,y)$ 没有含 y 的正次数公因式且没有单独一个 x 的正次数的公因式；因此它们在 $\Phi[x,y]$内除开单位外没有公因式．由此得 $f(x,y)$和 $g(x,y)$关于 x 的结式 $Q(y)$不是 0．设 V 是 C: $f(x,y)=0$ 和 D: $g(x,y)=0$ 在$\Omega^{(2)}$内的交，其中 $\Omega=\Phi(\sqrt{-1})$ 是Φ的代数闭包．如果 $(\rho,\sigma)\in V$，则由 $f(\rho,\sigma)=0=g(\rho,\sigma)$可推出 $R(\rho)=0$ 和 $Q(\sigma)=0$．因为 $R(x)\neq 0, Q(y)\neq 0$ 仅能给出有限多个可能的情形，故 V 是一个有限集．我们知道，如果 C 含有 $\Phi^{(2)}$ 的一点，则 V 有这样的一点，所以 $R(x)$ 在 Φ 中有一个根．反之，设 $R(x)$在 Φ 中有一个根．如果 α 不是含 x 的多项式的一个根，而这个多项式 $f(x, y)$中 y 的最高次方幂的系数，则由 $R(\alpha)=0$ 可推出使 $(\alpha,\sigma)\in V$ 的 $\sigma\in\Omega$ 的存在性．如果 $\sigma=\beta\in\Phi$，则我们得到了所要求的结果即 V 从而 C 在 $\Phi^{(2)}$中有一个根．否则，$(\alpha,\bar{\sigma})\in V$，其中 $\bar{\sigma}\neq\sigma$ 是 σ

的在 Ω/Φ 的自同构（≠1）下的共轭元。则我们在 V 中有两点：(α,σ)和$(\alpha,\bar{\sigma})$有相同的横坐标。

只要适当选择坐标轴，我们就容易克服我们曾经指出过的两个困难，这些困难妨碍我们断定如果 $R(x)$在Φ中有一个根，那么V因此C在 $\Phi^{(2)}$中有点。我们将改用 x',y' 系，其中 $x=\mu(x'+y'),y=y'$ 和$\mu\neq 0$是Φ中适当选取的，C在 x', y' 系中的方程是 $f(\mu(x'+y'),y')=0$. 设 $f_n(x,y)$是多项式 $f(x,y)$中含x和y的最高次 $n(>0)$的齐次部分，则 $f(\mu(x'+y'),y')$中$(y')^n$的系数是 $f_n(\mu,1)$. 因为 $f_n(x,1)\neq 0$,我们可选取$\mu\in\Phi$使得 $f_n(\mu,1)\neq 0$. 由于 $f(x,y)$的总次数是 n,由此得常数 $f_n(\mu,1)\neq 0$是含 x' 的多项式，它是 $f(\mu(x'+y'),y')$中 y' 的最高次幂的系数。这就克服了一个困难. 为克服另一个困难，把欧几里得算法用于$R(x)$和 $R'(x)$,我们求一个有单根的多项式 $r(x)$，它与 $R(x)$有相同的单根. 类似地，我们求与 $Q(y)$有相同单根的多项式 $q(y)$。接着我们可以求出多项式 $s(x)$，它的根为 $(\rho_i-\rho_{i'})(\sigma_j-\sigma_{j'})^{-1}$，其中 $\rho_1,\cdots,\rho_s$ 是 $r(x)$的根，$\sigma_1,\cdots,\sigma_t$ 是 $q(y)$的根，$i\neq i'$，$j\neq j'$. 为此我们引进未定元 $\xi_i,1\leqslant i\leqslant s,\eta_j,1\leqslant j\leqslant t$，并考察多项式

$$\prod_{\substack{i\neq i'\\ j\neq j'}}[(\eta_j-\eta_{j'})x-(\xi_i-\xi_{i'})].$$

在ξ和η的所有置换作用下这是不变的，所以x的方幂的系数是诸ξ和诸η的初等对称多项式的整系数多项式（卷 1，中译本 p.102）. 如果我们把 $r(x)$和 $q(y)$正规化到首项系数为 1 并用其相应的系数代替这些初等对称多项式，就得到一个多项式 $s(x)$，它的根是$(\rho_i-\rho_{i'})(\sigma_j-\sigma_{j'})^{-1},i\neq i'$，$j\neq j'$. 现设$\mu$不是 $s(x)$的根(也不是 $f_n(x,1)$ 的根)并考察点(ρ_i,σ_j)的集. 这个集包含V而且由于 x', y' 系中(ρ,σ)是点$(\mu^{-1}\rho-\sigma,\sigma)$故在此集中没有两个不同的点在 x', y' 系中有相同的横坐标，因此如果 $(i,j)\neq(i',j')$,那么就有 $\mu^{-1}\rho_i-\sigma_j\neq\mu^{-1}\rho_{i'}-\sigma_{j'}$.

现在我们按要求选取μ并用 $h(x,y)=f(\mu(x+y),y)$ 和

$k(x,y)=g(\mu(x+y),y)$ 代替 $f(x,y)$ 和 $g(x,y)$. 设 $f(x)$ 是 $h(x,y)$和 $k(x,y)$ 关于 y 的结式. 则论证表明 $f(x,y)=0$ 在Φ中是可解的当且仅当 $f(x)$ 在Φ中有根. 后一个问题可由斯图姆定理判定.

为了把此点推广到两个以上的变量，必须考察含有参数的多项式和应用归纳法. 这就需要扩充刚才我们所给定的判定法来研究受不等式 $g(x)\neq 0$ 限制的方程 $f(x, y)=0$. 为了掌握这个方法我们首先用欧几里得算法求出 $g(x)$和 $f(x,y)$中 y 方幂的系数的最高公因式 $d(x)$. 记 $f(x,y)=d(x)f_1(x,y)$, $g(x)=d(x)g_1(x)$. 则 $f(\alpha,\beta)=0$ 和 $g(\alpha)\neq 0$ 这一对条件等价于 $f_1(\alpha, \beta)=0$ 和 $g(\alpha)\neq 0$ 这一对条件. 这个陈述允许我们把所考察的情况归结为 $g(x)$和 $f(x,y)$设有正次数的公因式之情况. 为了避免考虑平凡的情况,我们还假设 $\deg g(x)>0$ 和 $\deg_x f(x,y)>0$. 设 $T(y)$是 $f(x,y)$和 $g(x)$关于 x 的结式,则 $T(y)\neq 0$, 因为否则 $f(x,y)$和 $g(x)$在 $\Phi(x,y)$ 中有关于 x 的正次数的公因式，这与我们所处理的情况矛盾. 于是在Φ中选取 τ 使得 $T(\tau)\neq 0$,并用 $h(x,y)=f(x,y+\tau)$代替 $f(x,y)$. 则 $h(x,y)$和 $g(x)$关于 x 的结式是 $T(y+\tau)$,当 $y=0$时 $T(y+\tau)\neq 0$. 由此得 $g(x)$和 $h(x,0)$互素. 为了判别 $f(x,y)=0$, $g(x)\neq 0$ 在Φ中解的存在性问题,显然我们可以用一对 $h(x,y),g(x)$代替 $f(x,y)$, $g(x)$这一对多项式. 现令 $k(x,y)=h(x,g(x)y)$. 则如果 (α, β) 满足 $h(\alpha,\beta)=0$, $g(\alpha)\neq 0$,则对于 $\gamma=\beta g(\alpha)^{-1}$我们有 $k(\alpha,\gamma)=0$. 另一方面,如果 $k(\alpha,\gamma)=0$, $h(\alpha,g(\alpha)\gamma)=0$,那么由于 $h(x,0)$和 $g(x)$互素则有 $g(x)\neq 0$. 因此α和 $\beta=g(\alpha)\gamma$ 满足$h(\alpha,\beta)=0$, $g(\alpha)\neq 0$. 这说明 $f(x,y)=0$, $g(x)\neq 0$ 在 $\Phi^{(2)}$中有解 (α,β) 当且仅当 $k(x,y)=0$ 在 $\Phi^{(2)}$中有解，而这就是我们在前面所处理的情形.

9. 带参数的方程 如果我们想把上一节所给出的方法推广到两个以上的变量,我们就会想到把所有变数除两个外都作为参数,而且去探求利用此方法以减少变量的个数. 这就导致考察包含参

数的多项式．由于允许参数在实闭域中取任意一个值，不失一般性可设多项式的系数为有理数．而且，我们用这种方法所得到的结果无例外地可应用到一切实闭域，并能用它建立一个属于塔尔斯基的重要原则，即代数的任一初等命题（必须使这一概念更为精确）对一个实闭域正确，那么它对所有的实闭域也正确．处理这些问题的赛登堡方法之主要结果是下述的

定理 15. 设 $F(t_i;x,y)\in R_0[t_1,\cdots,t_r;x,\ y]$，$G(t_i;x)\in R_0[t_1,\cdots,t_r;x]$，$t_i,x,y$ 是未定元，R_0 为有理数域．则我们可以通过有限步决定一个多项式对有限集 $(F_j(t_i;x),\ G_j(t_i))$，$F_j\in R_0[t_i;x]$，$G_j\in R_0[t_i]$，$j=1,2,\cdots,h$，使得，如果 Φ 是任一个实闭域，则 $\tau_i\in\Phi(1\leqslant i\leqslant r)$ 具有以下性质：

(21) $$F(\tau_i;x,y)=0,\ G(\tau_i;x)\neq 0,$$

对 $x,y\in\Phi$ 是可解的当且仅当对 Φ 中的 x，

(22) $$G_j(\tau_i)\neq 0\ \text{和}\ F_j(\tau_i;x)=0$$

是可解的．

此定理的证明本质上是上一节判定方法的形式化．我们首先考虑某些必要的预备概念．

我们将称 r 元组 $(\tau_1,\tau_2,\cdots,\tau_r)$ 的集 $\Phi^{(r)}(\tau_i\in\Phi)$ 为参数空间．称 $\mathfrak{U}=R_0[t_i]$ 的有限子集对 (δ_j,λ_j) 的有限集 $(j=1,2,\cdots,h)$ 为一个有理覆盖，如果对任一个特征为 0 的 Φ，$\Phi^{(r)}$ 是集 S_j 的并，而 S_j 是由 (δ_j,λ_j) 定义的，即 S_j 是 $\Phi^{(r)}$ 中使得 $d(\tau_i)=0$，$d\in\delta_j$，$l(\tau_i)\neq 0$，$l\in\lambda_j$ 的元 (τ_i) 的集．如果 $(\delta_j',\ \lambda_j')$，$j=1,\cdots,\ h$，(δ_k'',λ_k'')，$k=1,\cdots,q$ 是有理覆盖，则 $(\delta_j'\cup\delta_k'',\ \lambda_j'\cup\lambda_k'')$，$j=1,\cdots,h$，$k=1,\cdots,q$ 也是．相应的集是两个给定有理覆盖的交．我们将称此集为两个有理覆盖的加细．

我们知道，如果 $F=a_nx^n+\cdots+a_0$，$G=b_mx^m+\cdots+b_0$，$a_j,b_j\in R_0[t_i]$，$a_n\neq 0$，$b_m\neq 0$，$n\geqslant m$，则我们有一个唯一确定的带余除法算法，可得出一个偶数 $e\geqslant n-m+1$ 和 $R_0[t_i;\ x]=\mathfrak{U}[x]$，$\mathfrak{U}=R_0[t_i]$ 中的一个商式 Q 及一个余式 R，使得 $b_m^eF=QG-R$，其中 $\deg_xR<\deg_xG$．这可推广到 $n<m$ 或 $F=0$

的情形，只要取 $e=0$，$Q=0$，$R=-F$ 就行了．与多项式对 (F,G) 相联系的有若干个**一般欧几里得序列** $F_0,F_1,\cdots,F_s$，它们是由下述规则决定的：F_0 和 F_1 是 F 和 G 或者是从 F 和 G 分别去掉开头的一些项而得到的．因此 $F_0=a_px^p+\cdots+a_0$，其中 $0\leqslant p\leqslant n$，$F_1=b_qx^q+\cdots+b_0$，$0\leqslant q\leqslant m$．如果 $F_1=0$，我们取 $S=0$，而且令此序列仅由 F_0 组成．否则，用 F_1 除 F_0，而且令 F_2 是它的余式或者是从余式去掉开头的一些项的一个多项式．如果 $F_2=0$，则序列到 F_0,F_1 终止；否则，再重复此过程．显然，由于对每个 F_k 仅有有限多种选择，此过程经过有限步后必中断，我们就为 (F,G) 得到了有限多个一般欧几里得序列 E．令 $D(t_i;x)=F_s(t_i;x)$ 是序列 E 的最后一项．则 $D\neq 0$，除非 $F_0=F_1=0$，除了这种情形，我们可以用 D 除 F 和 G 得出 $m(t_i)^eF=F^{(1)}D-R^{(1)}$，$m(t_i)^fG=G^{(1)}D-S^{(1)}$，其中 $m(t_i)$ 是 D 的首项系数，e 和 f 是偶数，而在此除法中得到的商式是 $F^{(1)},G^{(1)}$，余式是 $R^{(1)},S^{(1)}$．与每个 E 相关联的是 $R_0[t_i]$ 的子集对 $(\delta(E),\lambda(E))$，其中 $\delta(E)$ 是在形成的过程中被去掉的项之系数所成的集（即 $F-F_0$ 和 $G-G_0$ 的系数），$\lambda(E)$ 是 F_k 的首项系数的集．

现设 Φ 是任一个特征为 0 的域，$(\tau_i)\in\Phi^{(r)}$，并设 $f(x)=F(\tau_i;x)$，$g(x)=G(\tau_i;x)$．易知存在对 (F,G) 的一般欧几里得序列 E 使得对一切 $d\in\delta(E)$，$d(\tau_i)=0$，对一切 $l\in\lambda(E)$，有 $l(\tau_i)\neq 0$．故对所有的一般欧几里得序列 E，对 $(\delta(E),\lambda(E))$ 的集是一个有理覆盖．如果 E 关于 (τ_i) 如所指出的那样选出，则 $d(x)=D(\tau_i;x)$ 是 $f(x)$ 和 $g(x)$ 在 $\Phi[x]$ 内的最高公因式，而且如果 $D(t_i;x)\neq 0$，我们有多项式 $F^{(1)}(t_i;x)$，$G^{(1)}(t_i;x)$ 使得 $m(\tau_i)^e f(x)=d(x)f_1(x)$，$m(\tau_i)^f g(x)=d(x)g_1(x)$，其中 $f_1(x)=F^{(1)}(\tau_i;x)$，$g_1(x)=G^{(1)}(\tau_i;x)$，而 $m(t_i)$ 是 $D(t_i;x)$ 的首项系数．由于 $m(t_i)\in\lambda(E)$，我们有 $m(\tau_i)\neq 0$．

有一条明显的途径可以把刚才我们所指出的程序推广到任意有限多个多项式的集．我们还将需要对于两个未定元 x，y（除 t_i 以外）的多项式给出程序．我们在 $\mathfrak{A}[x,y]=R_0[t_i;x,y]$ 中与

$F(t_i;x,y)$和 $G(t_i;x,y)$开始,并把 x 看成是 t_i 中的一个. 关于 y 的带余除法给出了 $l(t_i;x)^e F = QG - R$,其中 $\deg_y R < \deg_y G$. 如果我们注意到对 $d(t_i;x) \in R_0[t_i;x]$的一个关系式 $d(\tau_i;x) = 0$ 等价于对于 $d(t_i;x)$的所有系数 $d_k(t_i)$有 $l_k(\tau_i) = 0$, 以及 $l(\tau_i;x) \neq 0$, $l(t_i;x) \in R_0[t_i;x]$, 成立当且仅当对于某个系数 l_k 有 $l_k(\tau_i) \neq 0$,就知道我们可以决定一个有理覆盖 (δ_j,λ_j), $j = 1,2,\cdots,h$,和多项式 $D_j(t_i;x,y)$以及 $F_j^{(1)}(t_i;x,y)$, $G_j^{(1)}(t_i;x,y)$(如果 $D_j \neq 0$),使得如果(τ_i)是在由(δ_j,λ_j)所决定的子集 S_j 内,则 $d(x,y) = D_j(\tau_i;x,y)$是 $f(x,y) = F(\tau_i;x,y)$和 $g(x,y) = G(\tau_i;x,y)$ 在 $\Phi(x)[y]$中的一个最高公因式. 而且, 如果 $D(t_i;x,y) \neq 0$, $m(t_i;x)$是把D作为 y 的多项式的首项系数,则 $m(x) = m(t_i;x) \neq 0$ 且 $m(x)^e f(x,y) = d(x,y) f_1(x,y)$, $m(x)^f g(x,y) = d(x,y) g_1(x,y)$,其中 $f_1(x,y) = F_j^{(1)}(\tau_i;x,y)$, $g_1(x,y) = G_j^{(1)}(\tau_i;x,y)$.

还有一种手法是我们所需要的, 它将取代在判定法中选择 Φ 中元 γ 的步骤, γ 满足: 对给定多项式 $f(x) \neq 0$ 有 $f(\gamma) \neq 0$. 设 $F(t_i;x) = F_q(t_i)x^q + \cdots + F_0(t_i)$,其中 $F_q(t_i) \neq 0$. 首先设(τ_i)在 $\Phi^{(r)}$ 内满足 $F_q(\tau_i) \neq 0$. 如果我们记起在 §3 中关于给定多项式在Φ内根的界,就知道 $\eta = (q+1) + \sum_0^{q-1} F_k(\tau_i)^2 F_q(\tau_i)^{-2}$ 不是 $F(\tau_i;x)$的根. 因此, 如果我们令 $Q(t_i) = (q+1) F_q(t_i)^2 + \sum_0^{q-1} F_k(t_i)$, $P(t_i) = F_q(t_i)^2$,则对一切满足 $F_q(\tau_i) \neq 0$ 的(τ_i)有 $P(\tau_i) \neq 0$, $Q(\tau_i) \neq 0$,而且 $\eta = Q(\tau_i)P(\tau_i)^{-1}$ 不是 $F(\tau_i;x)$的根. 其次设 $F_q(\tau_i) = 0$ 并对 $F_q(t_i)$ 后的第一个不为 0 的系数 $F_p(t_i)$有 $F_p(\tau_i) \neq 0$. 则我们可以用 p 代替 q 重复上述讨论. 如此继续下去就得到一个有理覆盖 (δ_j,λ_j), $j = 1,2,\cdots,h$, 使得对于 $(\tau_i) \in S_h$ 有 $F(\tau_i;x) = 0$, 而对于 $j < h$ 有 $P_j(t_i)$, $Q_j(t_i)$使得对于 $(\tau_i) \in S_j$ 有 $P_j(\tau_i) \neq 0$, $Q_j(\tau_i) \neq 0$ 和 $F(\tau_i;Q_j(\tau_i)P_j(\tau_i)^{-1}) \neq 0$.

现在我们准备给出

定理 15 的证明 我们首先注意要证明定理只要给出一个有理覆盖(δ_k, λ_k)，$k = 1, \cdots, m$，使得对每个 k，可确定多项式对$G_{kj}(t_i) \in R_0[t_i]$，$F_{kj}(t_i; x) \in R_0[t_i; x]$的有限集具有以下性质：如果 $(\tau_i) \in S_k, S_k$ 是由(δ_k, λ_k)所定义的 $\Phi^{(r)}$之子集，则 $F(\tau_i; x, y) = 0$，$G(\tau_i; x) \neq 0$ 在Φ内是可解的当且仅当下列条件之一满足：$G_{kj}(\tau_i) \neq 0$，$F_{kj}(t_i; x) = 0$ 在Φ中是可解的．如果有此情况，我们令 $F^*_{kj}(t_i; x) = F_{kj}(t_i; x)^2 + \sum_{d \in \delta_k} d(t_i)^2$，$G^*_{kj}(t_i) = G_{kj}(t_i) \prod_{l \in \lambda_k} l(t_i)$．则多项式对$(F^*_{kj}(t_i; x)$，$G^*_{kj}(t_i))$ 的有限集满足定理的命题中多项式对 $(F_j(t_i; x), G_j(t_i))$的集所满足的条件．

其次我们考虑把定理由一对条件 $F(t_i; x, y) = 0, G(t_i; x) \neq 0$ 简化成单一条件 $F(t_i; x, y) = 0$.（这对应于上一节讨论中的后一半的内容）.我们将对 $\deg_x F$ 用归纳法，而且注意到若F不包含x则此结论是显然的．这时我们可以取 $F(t_i; x)$ 是以消失的x替代y而得到的多项式，并取 $G(t_i)$是 $G(t_i; x)$的系数的平方和．现设$\deg_x F(t_i; x, y) > 0$，并把关于最高公因式的研究用到 $G(t_i; x)$和$F(t_i; x, y)$中y的方幂之系数上去．于是，得到一个有理覆盖使得对此覆盖的每一个元(δ, λ)都可以决定有理系数多项式 $m(t_i)$，$D(t_i; x), F^{(1)}(t_i; x, y)$，$G^{(1)}(t_i; x)$ 使得 $D(\tau_i; x)$ 是 $G(\tau_i; x)$ 和 $F(\tau_i; x, y)$中y项系数的最高公因式，而 $m(\tau_i) \neq 0$，

$$m(\tau_i)^e F(\tau_i; x, y) = D(\tau_i; x) F^{(1)}(\tau_i; x, y),$$
$$m(\tau_i)^f G(\tau_i; x) = D(\tau_i; x) G^{(1)}(\tau_i; x)$$

对由(δ, λ)定义的集S中的所有的(τ_i)成立．我们可以在集S中用一对 $F^{(1)}(t_i; x, y)$，$G^{(1)}(t_i; x)$代替 $F(t_i; x, y)$，$G(t_i; x)$，因此如果 $\deg_x F^{(1)} < \deg_x F$ 就可以用归纳法了．故可设所指出的次数相等，这意味着有 $\deg_x D = 0$，则 $D(t_i; x) = m(t_i)$，$G(\tau_i; x)$和$F(\tau_i; x, y)$ 的系数互素．于是令 $T(t_i; y)$是 $F(t_i; x, y)$和 $0x + G(t_i; x)$关于x的结式，故对于所有的 $(\tau_i) \in S$ 有 $T(\tau_i; y) \neq 0$，并通过有理覆盖的加细还可以设我们能找到 $P(t_i), Q(t_i) \in R_0[t_i]$

使得对 $(\tau_i)\in S$ 有 $\mathrm{P}(\tau_i)\neq 0$，$Q(\tau_i)\neq 0$，和 $T(\tau_i;Q(\tau_i)\mathrm{P}(\tau_i)^{-1})\neq 0$。我们用 $H(t_i;x,y)=\mathrm{P}(t_i)^f F(t_i;x,y+Q(t_i)\mathrm{P}(t_i)^{-1})$代替 $F(t_i;x,y)$，其中 $f=\deg_y F(t_i;x,y)$。$H(t_i;x,y)$和 $G(t_i,x)$关于 x 的结式有形式 $\mathrm{P}(t_i)^g T(t_i;y+Q(t_i)\mathrm{P}(t_i)^{-1})$，而且对于 $(\tau_i)\in S, y=0$，它是不等于 0 的。由此得 $H(\tau_i;x,y)=0$，$G(\tau_i;x)\neq 0$ 在 Φ 内可解当且仅当 $K(\tau_i;x,y)=0$ 在 Φ 内可解，这里 $K(t_i;x,y)=H(t_i;x,G(t_i;y)y)$。

现在我们考察单独一个方程 $F(t_i;x,y)=0$。通过考察 F 中 y 的方幂之系数的最高公因式，我们可以把研究简化为研究由一个有理覆盖所定义的子集 S 和多项式 $F(t_i;x,y)$使得对 $(\tau_i)\in S$，$F(\tau_i;x,y)$不能被 x 的正次数多项式所整除。下面，我们考虑 F 和 $\dfrac{\partial F}{\partial y}$ 的最高公因式，而且在加细之后，可以假设确定了有理系数多项式 $m(t_i;x)$，$D(t_i;x,y)$，$F_1(t_i;x,y)$使得 $D(\tau_i;x,y)$是 $F(\tau_i;x,y)$和 $\dfrac{\partial}{\partial y}F(\tau_i;x,y)$在 $\Phi(x)[y]$中的一个最高公因式，$m(\tau_i;x)\neq 0$ 和 $m(\tau_i;x)^e F(\tau_i;x,y)=D(\tau_i;x,y)F_1(\tau_i;x,y)$。则 $F_1(\tau_i;x,y)$没有含 y 的正次数的重因式，而且 F 和 F_1 在 $\Phi[x,y]$ 中有相同的含 y 的正次数不可约因式。我们还可以决定 $k(t_i)$，$L(t_i;x)$，$F_2(t_i;x,y)$使得 $k(\tau_i)^f F_1(\tau_i;x,y)=L(\tau_i;x)F_2(\tau_i;x,y)$，其中 $F_2(\tau_i;x,y)$不能被含 x 的正次数多项式所整除，则显然可以用 F_2 代替 F，而且可以设对 $(\tau_i)\in S$ 时 $F(\tau_i;x,y)$ 没有含 y 的正次数的重因式和没有单独一个 y 的正次数的因式。则 $F(\tau_i;x,y)$和 $\dfrac{\partial}{\partial y}F(\tau_i;x,y)$没有正次数的公因式。令 $G(t_i,c;x,y)=y\dfrac{\partial F}{\partial x}-(x-c)\dfrac{\partial F}{\partial y}$，其中 c 是另外的未定元，并设 $R(t_i,c;x)$ 是 $G(t_i,c;x,y)$和 $F(t_i;x,y)$ 关于 y 的结式。则我们如同证明判定法一样可以证明 $R(\tau_i,c;x)\neq 0$。通过把有理覆盖加细，我们可以得到 $\mathrm{P}(t_i)$，$Q(t_i)\in R_0[t_i]$ 使得 $\mathrm{P}(\tau_i)\neq 0$，$Q(\tau_i)\neq 0$，

$R(\tau_i, Q(\tau_i)P(\tau_i)^{-1}; x) \neq 0$. 如果我们用 $G(t_i; x, y) = P(t_i)G(t_i, Q(t_i)P(t_i)^{-1}; x, y)$代替 $G(t_i, c; x, y)$,可以看出 $F(t_i; x, y)$和 $G(t_i; x, y)$关于 y 的结式 $R(t_i; x)$对于 $(\tau_i) \in S$ 有 $R(\tau_i; x) \neq 0$. 与前面一样,我们也能证明F和G关于x的结式$Q(t_i; y)$满足 $Q(\tau_i; y) \neq 0$. 证明剩下的部分只要沿着判定法自身的线索就可以完成,我们把它留给读者.

10. 广义斯图姆定理 · 应用 现在我们可以证明下述的斯图姆定理的推广,它是属于塔尔斯基的.

定理 16. 设φ是多项式方程和不等式的有限集,这些多项式方程和不等式的形式如 $F(t_1, \cdots, t_r; x_1, \cdots, x_n) = 0$, $G(t_1, \cdots, t_r; x_1, \cdots, x_n) \neq 0$ 或者 $H(t_1, \cdots, t_r; x_1, \cdots, x_n) > 0$,其中 $F, G, H \in R_0[t_1, \cdots, t_r; x_1, \cdots, x_n]$. 则经过有限步就可以决定仅关于参数 t_i 的有相同类型的多项式方程和不等式之有限集 ϕ_j 的一个有限集族使得,如果Φ是任一实闭域,则集φ对Φ中的诸 x,对 $t_i = \tau_i$ $(1 \leqslant i \leqslant r)$ 有解当且仅当 τ_i 满足某一集 ϕ_j 的所有条件.

证. 我们首先证明可以简化组φ为形如 $F(t_i; x_j) = 0$ 的单一方程,其中诸x的个数可以增加: 首先,显然有不等式$G \neq 0$等价于 $G^2 > 0$. 其次,我们可用等价方程 $z^2H - 1 = 0$ 代替不等式 $H > 0$,而z是另一个未定元. 最后可以用单一方程 $\sum F_i^2 = 0$ 代替一系列方程 $F_i = 0$. 这些考察表明我们可以把φ取为一个单一方程 $F(t_i; x_j) = 0$. 首先我们对x的个数n用归纳法证明能决定有限多个形如 $F_k(t_i; x) = 0$, $G_k(t_i) \neq 0$ 的方程集使得集 $\tau_1, \tau_2, \cdots, \tau_r, \tau_i \in \Phi$, 有性质: $F(\tau_i; x_j) = 0$ 对于诸x在Φ中是可解的当且仅当对某个 k, $G_k(\tau_i) \neq 0$ 和 $F_k(\tau_i; x) = 0$ 在Φ中是可解的. 对于 $n = 1$ 这是显然的,而对于 $n = 2$ 则是定理 15 的一个推论. 假设对 $n - 1 \geqslant 2$ 定理成立. 然后把 x_n 作为一个参数就可以断定能找到有限多个有理系数多项式对 $(F_k(t_i; x_n; x), G_k(t_i, x_n))$使得,如果 τ_i 和 $\xi_n \in \Phi$,则 $F(\tau_i; x_1, \cdots, x_{n-1}, \xi_n) = 0$ 对于 $x_1, \cdots, x_{n-1}$ 在Φ内是可解的当且仅当对某个 k, $G_k(\tau_i, \xi_n)$

$\neq 0$ 和 $F_k(\tau_i, \xi_n; y) = 0$ 在Φ中是可解的. 由定理 15,对每个 k 能找到有理系数多项式对 $(F_{kj}(t_i;x), G_{kj}(t_i))$ 的一个有限集使得 $F_k(\tau_i,x;y) = 0$, $G_k(\tau_i;x) \neq 0$ 在Φ中是可解的当且仅当对某个 j 有 $G_{kj}(\tau_i) \neq 0$ 和 $F_{kj}(\tau_i;x) = 0$ 在Φ中是可解的. 由此得多项式对 $(F_{kj}(t_i;x), G_{kj}(t_i))$ 满足对 $F(t_i;x_1,\cdots,x_n)$所要求的条件. 现把这些多项式记为 $(F_j(t_i;x), G_j(t_i))$. 对于每个 $F_j(t_i;x)$, 由 §7 中所考虑过的斯图姆定理的变形表明能找到一个含 t_i 的有理系数多项式方程和不等式的有限集使得它们被 $t_i = \tau_i \in \Phi$ 满足当且仅当 $F_j(\tau_i; x)$ 在Φ中是可解的. 如果我们把不等式 $G_j(\tau_i) \neq 0$ 加到每个集上就得到满足定理要求的集 ϕ.

现设有有理系数方程和不等式组, 它在一个实闭域 Φ_1 中有解. 显然我们可以引进参数并把我们的断言改换为:某个带有参数的有理系数的方程和不等式组对于参数的某些有理数值在Φ中有解. 则由定理16得到: 这些有理数值满足一个有理方程和不等式的某一确定集. 因此,如果Φ是任一其它实闭域,我们可以再应用定理16倒推回去得到: 原来的方程和不等式组在Φ中有解.

再说,假设我们有一个含参数的有理系数方程和不等式组,并设 Φ_1 为一个实闭域, 此方程和不等式组对参数在 Φ_1 中任意选定的值在 Φ_1 内是有解的, 则我们从定理 16 得到这等价于下述命题: 对参数在 Φ_1 中取值的每个集均满足方程和不等式有限集的一个确定的有限集族. 易知这可能转化为下述的等价命题: 对于参数,有理方程和不等式有限集的任一另外的有限集族在 Φ_1 中没有解. 前面的结果表明这一点对每个实闭域均成立. 因此我们看出原来的方程和不等式组对参数在Φ中的任意选定的值都在Φ中有解,其中Φ为任意的实闭域.

现在我们将考虑这些结果对可除代数一个重要定理的应用.

很久以前,在发现实闭域以前,弗罗贝尼乌斯证明了下述定理: 实数域 R 上的有限维可除代数只能是: (1) R自身,(2) $R(\sqrt{-1})$, (3) R 上的哈密顿四元数代数. 此定理的已知的诸证明都是代数的并对任意实闭域给出相同的结果. 此定理的初等证明读者可参

看狄克逊的《代数和它们的算术》(Algebras and Their Arithmetics), p.62. 现在我们去掉结合性的假设(此假设在本书中是一贯的)而考虑非结合代数. 这些代数定义为基域Φ上的一个向量空间, 在其中定义了乘法 xy 满足分配律并有规则 $\alpha(xy)=(\alpha x)y=x(\alpha y)$, $\alpha\in\Phi$. 这样一个有限维代数称为可除代数, 如果它没有零因子: 在此代数中, 由 $xy=0$ 推出 $x=0$ 或者 $y=0$. 除上述的例子外, 另一个非结合可除代数的重要例子是八元数的八维代数, 它是由凯利 (Cayley) 和格利弗 (Grave) 发现的. 实数的域上已知的有限维非结合可除代数的例子有 1,2,4 和 8 维的. 长期以来猜想这些就是仅有可能的维数, 而此点最终被波蒂 (Bott) 和米尔诺 (Milnor) 用深刻的拓扑思想所证实. 想把此证明转移到实闭域的情形将会十分困难. 而且,这也是不必要的,因为可以十分容易地从对实数域的有效性得到对任意实闭域的相应结果. 假定对实数域得到波蒂和米尔诺的结果,我们将证明如果 $h\neq 1$, $2,4,8,\infty$,而Φ是一个实闭域,则不存在Φ上的n维非结合可除代数. 为证明这点, 设$\mathfrak{A}$是Φ上的一个非结合的代数, 在Φ上有基 $(u_1,\cdots,u_n)$, 并设 $u_iu_j=\sum\gamma_{ijk}u_k$, 其中 $\gamma_{ijk}\in\Phi$. 如果 $x=\sum\xi_iu_i$, $\xi_i\in\Phi$, 则映射 $y\to xy$ 在$\mathfrak{A}$中是线性的, 它关于基 $(u_1,\cdots,u_n)$的矩阵是 (ρ_{jk}),而 $\rho_{jk}=\sum\limits_i\xi_i\gamma_{ijk}$. 使得 $xy=0$ 的 $y\neq 0$ 的存在等价于 $y\to xy$ 是一个奇异的线性变换, 而这种情形成立当且仅当 $F(\gamma_{ijk};\xi_i)\equiv\det(\rho_{jk})=0$. 为了证明 $\mathfrak{A}$ 不是一个可除代数我们必须证明: 存在一个 $x\neq 0$ 使得 $F(\gamma_{ijk};\xi_i)=0$.于是可看出,我们的断言等价于:设 $F(t_{ijk};x_i)=\det(\sum\limits_i x_it_{ijk})$, 它可看作为未定元 t_{ijk}, x_i 的有理系数多项式. 则对一切的取值 $t_{ijk}=\gamma_{ijk}\in\Phi$, 多项式和不等式组 $F(\gamma_{ijk};x_i)=0$, $\sum x_i^2\neq 0$ 在Φ中有解 $x_i=\xi_i$. 于是由波蒂-米尔诺定理,此点对实数域 $\Phi=R$是成立的. 故我们的结果表明对每个实闭域它也是成立的.

相同类型的另外例子是霍普夫 (Hopf) 的一个定理, 它论述实非结合交换可除代数的有限维数只能是 $n=1,2$. $\mathfrak{A}$ 的交换性

等价于条件：对一切 i, j 有 $\gamma_{ijk}=\gamma_{jik}$. 因此在上述的讨论中，对于 $i\leqslant j$，我们考虑未定元 t_{ijk}，而对于 $j>i$ 则规定 $t_{jik}=t_{ijk}$. 这样一来 $\det(\sum_i x_i t_{ijk})$ 是一个含未定元 $t_{ijk}(i\leqslant j)$ 的有理系数多项式. 剩下的讨论可以照搬过来并可证明霍普夫定理对所有实闭域均有效.

有一个一般的可用上述方法处理的有关实闭域的命题类，它们就是所谓的代数初等语句. 我们并不打算给出它们的精确定义，而是给读者去参考文献(见本章参考书目). 我们已经考虑的结果其实是下述**塔尔斯基一般原则**的特殊情况：任一代数的初等语句或者对一切实闭域是真的，或者对一切实闭域是假的.

习 题 53

1. 假定这个结果对实数域成立，证明：如果 Φ 是任一个实闭域，$F_1(x_1,\cdots,x_n)=0,\cdots,F_k(x_1,\cdots,x_n)=0$，其中诸 $F\in\Phi[x_1,\cdots,x_n]$，有解 $x_i=\xi_i\in\Phi$，则它有一个最靠近原点的解.

2. 对特征为 0 的代数闭域 Φ 和方程 $F(t_1,\cdots,t_r;x_1,\cdots,x_n)=0$，不等式 $G(t_1,\cdots,t_r;x_1,\cdots,x_n)\neq 0$ 的有限集，其中 $F, G\in R_0[t_i;x_j]$，证明定理16的类比. (提示：此定理的一个简单证明可以建立在一般欧几里得序列和下述简单的属于塔尔斯基的想法. 如果 $f(x), g(x)\in\Phi[x]$ 和 $\deg f>0$, $\deg g>0$，则 $f(x)=0$, $g(x)\neq 0$ 在 Φ 中有解当且仅当 $f(x)$ 不是 $g(x)^{\deg f(x)}$ 的一个因式).

3. 通过将相应的结果推广到 $I_p[t_i;x]$ $(I_p=I/(p))$ 的一般欧几里得序列，证明第 2 题的结论对特征 $p\neq 0$ 的 Φ 仍有效.

11. 实闭域的阿廷-施莱尔刻划 我们将证明属于阿廷和施莱尔的关于实闭域的一个漂亮刻划来结束对实闭域的讨论. 我们知道，如果 Φ 是一个不含 $\sqrt{-1}$ 的域而 $\Phi(\sqrt{-1})$ 是代数闭的，则 Φ 是实闭的(定理 6). 现在我们要证明

定理 17. 设 Ω 是一个代数闭域，Φ 是 Ω 的一个真子域，它在 Ω 中是有限余维的，则 Φ 是实闭的和 $\Omega=\Phi(\sqrt{-1})$.

证 设 $\Phi'=\Phi(\sqrt{-1})\subseteq\Omega$. 如果能证明 $\Phi'=\Omega$，则由引用的结论就可推出定理 17. 因此设 $\Omega\supset\Phi'$. 令 E 是 Φ' 的一个代数扩张，则 E 是同构于 Φ' 上 Ω 的一个子域，故 $[E:\Phi']\leqslant[\Omega:\Phi']$. 故 Φ 的诸代数扩张的维数都是有界的. 由此得 Φ' 是完全的，否

则其特征为 $p \neq 0$，并存在 $\beta \in \Phi'$ 不是 p 次幂. 则对每个 $e > 0$，$x^{p^e} - \beta$ 在 $\Phi'[x]$ 中是不可约的(§1.6，习题的第 1 题)，这就给出了 Φ' 上的一个 p^e 维的代数扩张. 由于 e 是任意的，这与我们已证明的结论矛盾，因此 Φ' 是完全的而 Ω 在 Φ' 上是可分的. 由于 Ω 是代数闭域，故它在 Φ' 上是伽罗瓦的，而且因为 $\Omega \supset \Phi'$，所以它在 Φ' 上的伽罗瓦群 $G \neq 1$，因此 G 含有一个素数 q 阶的循环子群，于是存在子域 $E \supset \Phi'$ 使得 Ω 在 E 上是 q 维循环的. 由于 Ω 是 E 的一个代数闭包和 $[\Omega:E] = q$，显然 Ω 和 E 是 E 的仅有的代数扩张. 由此可知 Φ 的特征不是 q. 否则，Ω 是 E 的循环 q 扩张，而由 E 的这样一个扩张的存在推出对每个 m，E 的循环 q^m 扩张的存在(定理 3.16). 这种情况已被排除，故其特征不是 q. 由此得代数闭域 Ω 有 q 个不同的单位根. 由于这些是 $(x-1)(x^{q-1} + x^{q-2} + \cdots + 1)$ 的根，而且因为 $E[x]$ 中不可约多项式的次数为 1 或 q，故 1 的所有 q 次根均含于 E 中. 因为 Ω 是 E 上循环 q 维的，故 $\Omega = E(\sqrt[q]{\alpha})$，其中 $\alpha \in E$，且在 E 中不是一个 q 次幂(定理2.5). 考虑多项式 $g(x) = \prod_{1}^{q^2} (x - \zeta^i \rho)$，其中 ζ 是本原 q^2 次单位根，而 ρ 是 Ω 中使得 $\rho^{q^2} = \alpha$ 的一个元. 由于由包含关系 $\zeta^i \rho \in E$ 可推出 E 包含一个元 $(\zeta^i \rho)^q = \beta$ 使得 $\beta^q = \alpha$，我们看出没有 $\zeta^i \rho \in E$. 因为 $g(x) = x^{q^2} - \alpha \in E[x]$，于是它在 $E[x]$ 内的所有不可约因式都是 q 次的. 如果 β 是一个不可约因式的常数项，则 $\beta = \rho^q \eta$，其中 η 是 ζ 的方幂. 因为 $(\rho^q)^q = \alpha$，而且 $\Omega = E(\sqrt[q]{\alpha})$，则 $\rho^q \notin E$，$\Omega = E(\rho^q) = E(\beta\rho^{-q}) = E(\eta)$. 由于 E 包含一切 q 次单位根，因此可看出 η 是一个本原 q^2 次单位根. 设 Φ_0 是 Ω 的素域，并考虑 Ω 的子域 $\Phi_0(\eta)$. 如果 Φ_0 是有理数域 R_0，则 q^r 次单位根的域的维数是 $\varphi(q^r)$(定理 3.2)，而且 $\varphi(q^r)$ 随 r 一起趋于无穷. 如果 Φ_0 有特征 $p \neq q$，则在 Φ_0 上 q^r 次单位根的域至少包含 q^r 个元，故此域在 Φ_0 上的维数趋于无穷. 于是在任何情形下都存在一个正整数 r 使得 $\Phi_0(\eta)$ 包含一个本原 q^r 次单位根而不是本原 q^{r+1} 次单位根. 因为 η 是一个本

原 q^r 次单位根，则 $r \geq 2$. 域 Ω 含有一个本原 q^{r+1} 次单位根，譬如说 ξ. 令 $h(x)$ 是 ξ 在 E 上的最小多项式. 由于 $\eta \notin E$, $\xi \notin E$, 那么 $\deg h(x) = q$. 又 $h(x)$ 是 $x^{q^{r+1}} - 1 = \prod_{j}^{q^{r+1}} (x - \xi^j)$的一个因式，则 $h(x)$的系数是包含在 $\Phi_0(\xi)$中；因此他们含于域 $\Gamma = \Phi_0(\xi) \cap E$ 中. 由此得出 $[\Phi_0(\xi):\Gamma] = q$. 其次，考虑 $\Phi_0(\xi)$ 的子域 $\Gamma' = \Phi_0(\gamma)$, $\gamma = \xi^q$. 显然γ是一个本原 q^r 次单位根，那么 Γ' 含有 q 个不同的 q 次单位根. 另一方面，$\Phi_0(\xi) = \Gamma'(\xi)$, 其中 $\xi^q = \gamma \in \Gamma'$,则 $\Phi_0(\xi) = \Gamma'$ 或者 $\Phi_0(\xi)$ 是 Γ' 上 q 维循环扩张. 如果 $\Phi_0(\xi) = \Gamma' = \Phi_0(\gamma)$,因为 $\Phi_0(\eta)$包含一切 q^r 次单位根，我们有 $\Phi_0(\xi) \subset \Phi_0(\eta)$. 则 $\Phi_0(\eta)$包含 ξ,而ξ为一个本原 q^{r+1} 次单位根，这与假定相矛盾. 因此我们得到 $[\Phi_0(\xi): \Gamma'] = q$. 于是 $\Gamma' \neq \Gamma$. 否则，Γ 包含一个本原 q^r 次单位根，那么Γ 和E 包含 η, 这与 $\Omega = E(\eta) \supset E$ 矛盾. 因此，我们证明了在素域上的 q^{r+1} 次单位根的域 $\Phi_0(\xi)$包含两个不同的子域Γ 和 Γ',$\Phi_0(\xi)$在它们上的维数为 q. 由此得 $\Phi_0(\xi)$ 在 Φ_0 上的伽罗瓦域不是循环的. 由§1.13 的引理 1 和定理 3.5，这只有在特征为 0 且 $q = 2$ 时才会出现. 所以前面考虑的 η 是一个本原 4 次 (q^2, 而 $q = 2$) 单位根. 另一方面，E 包含 Φ',它包含$\sqrt{-1}$,而这是一个本原 4 次单位根. 因此我们有 $\Omega = E(\eta) = E$, 与$\Omega \supset E$ 矛盾. 此矛盾表明 $\Phi' = \Phi(\sqrt{-1}) = \Omega$ 而且 Φ 是实闭域.

参 考 书 目

第一章 在自同构群和子域之间的古典伽罗瓦对应已发展成若干不同的方向. 首先，在第六章考虑了克鲁尔无穷维扩张伽罗瓦理论. 其次，还有可除环的伽罗瓦理论，这是被 H. 嘉当 (Cartan) 和本书著者独立发现的. 这方面的内容可以在著名的 Structure of Rings 的第七章 (A. M. S. Colloquium Vol. 37 (1956)) 中找到. (第一章中展开的伽罗瓦理论是建立在最初为了处理非交换

(环)论发展起来的那些方法的基础之上的.)有限维可分扩张的伽罗瓦理论基于域的自表示的概念，它属于卡罗杰林 (Kalouinine).这个内容包含在著者在下列两篇文章中所阐述的更一般的理论之中：*Am. J. Math.* Vol. 66(1944), pp. 1—29 和 pp.636—644.也可参考霍赫希尔德和丢东勒 (Dieudonné) 在同一个杂志上发表的两篇文章，Vol. 77 (1949), pp. 443—460 和 Vol. 73(1951), pp. 14—24.

最近，交换环的自同构的伽罗瓦理论被 S. U. 蔡斯 (Chase), D. K. 哈利逊 (Harrison) 和 A. 罗森堡 (Rosenberg) 共同发展了．此文发表在 Transactions A. M. S. 中.

域的一般上同调理论由阿米策 (Amitsur) 所给出，发表在 Trans. A. M. S., Vol.90(1959), pp. 73—112. 也可参考罗森堡和柴林斯基 (Zelinsky) 关于这一课题的文章 (Trans. A. M. S., Vol. 97(1960), pp. 327—356) 和阿米策的文章 J. Math. Soc. Japan, Vol. 14(1962), pp. 1—25.

第二章 本书曾指出，对于给定的域Φ和一个给定的有限群G,是否存在伽罗瓦扩张 P/Φ 使其伽罗瓦群同构于G是一个未解决的问题．与此紧密相关的问题是：是否存在系数在Φ中的方程以给定的 S_n 的子群作为群．这些问题对于Φ是有理数域和更一般地对代数数域(有理数域的有限维扩张)已被广泛的研究．对这个问题发展了两种方法：一种建立在数域的算术性质之基础上，而第二种更初等的方法基于希尔伯特的不可约准则．迄今在数论中最好的结果是属于沙发雷维奇 (Šafarevič) 的．他的结果的摘要发表在 Math. Reviews, Vol. 16(1955), pp.571—572.

希尔伯特方法(希尔伯特用来证明以 S_n 为伽罗瓦群的有理方程的存在性)分为两步．给定域 Φ,我们首先要求一个纯超越扩张域 $\Phi(t_1,\cdots,t_r)$ 和 $\Phi(t_i)$ 的一个伽罗瓦扩张 P,其伽罗瓦群同构于给定的群 G. 这个问题除开特殊情况外 (S_n, 交错群和某些其它群) 仍是没有解决的．其次，我们需要知道Φ是一个希尔伯特域，即在Φ中希尔伯特不可约定理成立.(例如，有理数域是希尔伯

特域；p-adic 数域和有限域都不是）. S. 朗格 (Lang) 的书《Diophantine Geometry》(纽约，1962，第八章)讨论了这一定理及其与伽罗瓦理论的关系.

方程的古典伽罗瓦理论的一个有趣的方面是形式问题的克莱因 (K. Lein) 理论. 此问题从代数的观点，特别是从交叉乘积出发的发展是属于 R. 布劳尔 (Brauer) 的 (Math. Annalen, Vol. 110(1934), pp. 437—500). 这篇文章给出了关于这个内容的经典工作的参考材料.

对于方程的伽罗瓦理论的一般参考书是切波塔略夫 (Tschebotaröw) 的《Grundzüge der Galoisschen Theorie, Groningen》, 1950 (由 Schwerdtfeger 译自俄文).

第三章 D. K. 哈利逊已给出交换扩张域的一般理论(Trans. A. M. S., Vol. 106(1963), pp. 230—235).

第四章 本章的某些较深入的结果已发展到为满足代数几何的需要服务. 对于这些内容的联系读者可以参阅 S. 朗格的《Introduction to Algebraic Geometry》, 1958, 或者 A. 韦尔 (Weil) 的《Foundations of Algebraic Geometry》, A. M. S. Colloquium, Vol.29, Providence, 1946 年第一版，1962年第二版.

第五章 要继续钻研本章的主要课题可以沿着若干方向进行. 首先，我们可以研究赋值的一般理论，可参考沙利斯基-萨姆尔 (Zariski-Samual) 的《Commutative Algebra》之卷 II, 第六章 (Van Nostrand 有限公司，Princeton, 1960). 第二，这一章导致了数域和一个变量的代数函数域的算术理论. 为此，读者可以参考车佽利 (Chevalley) 的书《Algebraic Functions of One Variable》(Princeton, 1960)，阿廷的书《Theory of Algebraic Numbers》(Göttingen, 1959) 及 E. 怀斯 (Weiss) 的书《Algebraic Number Theory》(New York, 1963). 在研究了第五章以后，我们可以继续钻研的第三个方向是局部类域论. 对此，读者可以参考塞雷 (Serre) 的书《Corps Locaux》(Paris, 1962).

第六章 最初的阿廷-施莱尔理论出现在阿廷和施莱尔的文

章中以及阿廷在《Hamburg Abhandl》(Vol. 5, 1927) 中的工作，我们的叙述与这些文章比较接近。赛登堡的工作见于 Annals of Math., Vol. 60(1954), pp. 365—374. 此文中还有塔尔斯基原理的命题，当然，也有关于塔尔斯基较早的文章参考材料。本章的大部分内容可以作为数理逻辑的一部分，更确切些，可作为模型论的一个方面来展开。读者可以参考 A. 罗宾逊 (Robinson) 的书《Model Theory》(Amsterdam, 1963)，特别是第八章。这本书也给出了参考文献。

术 语 索 引

六 划

七 划

八　划

九　划

十　划

十一划

十二划

十三划以上

其 它

［Ｇｅｎｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ］
书名＝数学名著译丛　　抽象代数学　卷３　域论及伽罗瓦理论
作者＝
页数＝３１５
ＳＳ号＝０
出版日期＝